Schule ans Netz

Infrastruktur, aber frei, offen, datenschutzkonform und sicher

Sven Freitag (sven.freitag@st.ovgu.de)
Lukas Kummer (lukas.kummer@st.ovgu.de)
Anonymus

Technische Aspekte in der IT-Sicherheit

Fakultät für Informatik
Otto-von-Guericke-Universität Magdeburg

1. Diskussionsrunde 1, 17. April 2019
2. Diskussionsrunde 2, 29. Mai 2019
3. Diskussionsrunde 3, 26. Juni 2019

Folien auch unter `http://www.ovgu.de/svfreita/` verfügbar.

Schule heute: Was ist gewünscht? (SF)

- Computer-Arbeitsplätze
- Nutzung eigener Geräte (BYOD)
- Dateispeicher, der auch zuhause nutzbar ist
- Kommunikationsplattformen zwischen Schülern, Lehrern, Eltern
- Vertretungsplan, Raumplan, Terminplan, Zensurverwaltung, ...

Wie sieht es bisher aus? (SF)

- Arbeitsplätze: Windows (M$-Rahmenvertrag)
- Dateispeicher: Dropbox, Google
- Kommunikationsplattform: Whatsapp, Facebook, unsichere E-Mail
- Verwaltung: $proprietär ???

Warum ist das schlecht? (SF)

- Überwachung: Windows 10 sendet Daten an M$, Facebook/Whatsapp legen Profile an
- Ressourcen: Windows schluckt Ressourcen (Hardware UND Personal)
- Abhängigkeit: Rahmenverträge knebeln Schulen, Anbieter kann Support einstellen
- fehlende Freiheit für den Nutzer: Kaum Anpassungen des UI möglich
- Kosten: Lizenzverträge, Volumenlizenzen
  LiMux konnte IT-Kosten deutlich senken

Es gibt keine Gründe, proprietäre Software/Anbieter zu fördern!

Linuxmuster (SF)

- Komplettlösung zum Betrieb schulischer IT-Infrastruktur
- Ursprünglich: Einheitliche Infrastruktur in BaWü
- Entwickelt vom Verein linuxmuster.net e.V.
- Ubuntu LTS als Basis
- Deutschlandweit ca. 25465 Clients, ca. 135787 User
- Frei verfügbar (Open Source), keine Aktivierung nötig

Was bringt Linuxmuster mit? (SF)

- Imagingsystem LINBO → PXE-Boot der Clients
- Webbasierte grafische Benutzeroberfläche (Schulkonsole)
- Pädagogische Funktionen
- Schulspezifische Benutzerverwaltung
- Mailserver
- Cloud-Anbindung, moodle-Anbindung
- Raumbuchungssystem, Schulportfolio (OSP), Druckquotierung (Pykota)
- RADIUS, IPFire, VLAN-Unterstützung
- Erweiterungen: TOR, TrueCrypt/VeraCrypt
- ...

Was müssen wir hinzufügen/ändern? (LK/SF)

In Anlehunung an den Kompass Digitalisierung

- Unrat, den Ubuntu mitbringt, ersetzen/entfernen
- 2FA integrieren
- XMPP-Server
  Warum? Damit keiner erst anfängt, Whatsapp vorzuschlagen
- YaCy zur Suche im Intranet/Internet
- Anpassung der Anwendersoftware, z.B.
  - Firefox/Palemoon: uBlock origin und uMatrix hinzufügen, Unrat deaktivieren, ...
  - Thunderbird: HTML-Mails als plain anzeigen, Header anzeigen, ...

Zu unterstützende Plattformen (SF)

- Arbeitsplätze: diskless fat clients, booten per PXE
  Es muss nur ein System gepflegt werden!
  `$HOME` über SSHFS (Performance?)
- BYOD: sehr heterogen (Linux, Android, . . .)
- Sollen Windows oder MacOS Beachtung finden?
  Pädagogik sagt NEIN
- Multimedia: Whiteboards, Grafiktabletts
- Barrierefreiheit: Braillezeilen

Daten, Lernplattformen, Kommunikation (SF)

- Nextcloud: Schüler und Lehrer sollen Daten auch zuhause nutzen können
  - Einfach zu bedienen
  - Stellt Gruppenverzeichnisse bereit, erlaubt Freigaben
  - LDAP-Anbindung vorhanden: Nutzer/Gruppen werden übernommen
  - Unterstützt 2FA
  - Synchronisation mit `$HOME`
- Moodle als Lernplattform (hat sich bewährt)
- MediaWiki?
- Mailserver zur Kommunikation zwischen Lehrern und Schülern
- XMPP als Instant-Messenger

Anwendungen für Schüler (LK/SF)

- Web: Firefox ESR oder Palemoon, Mail: Thunderbird, XMPP: Gajim+OMEMO
- Office/Text: Libreoffice, TEXlive
- Multimedia: GIMP, Inkscape, Audacity, Kdenlive, MPlayer, ...
- Fülle an Lernsoftware der KDE-Community
- Programmierung: Arduino, BlueJ, Lazarus, ...
- Barrierefreiheit: Orca

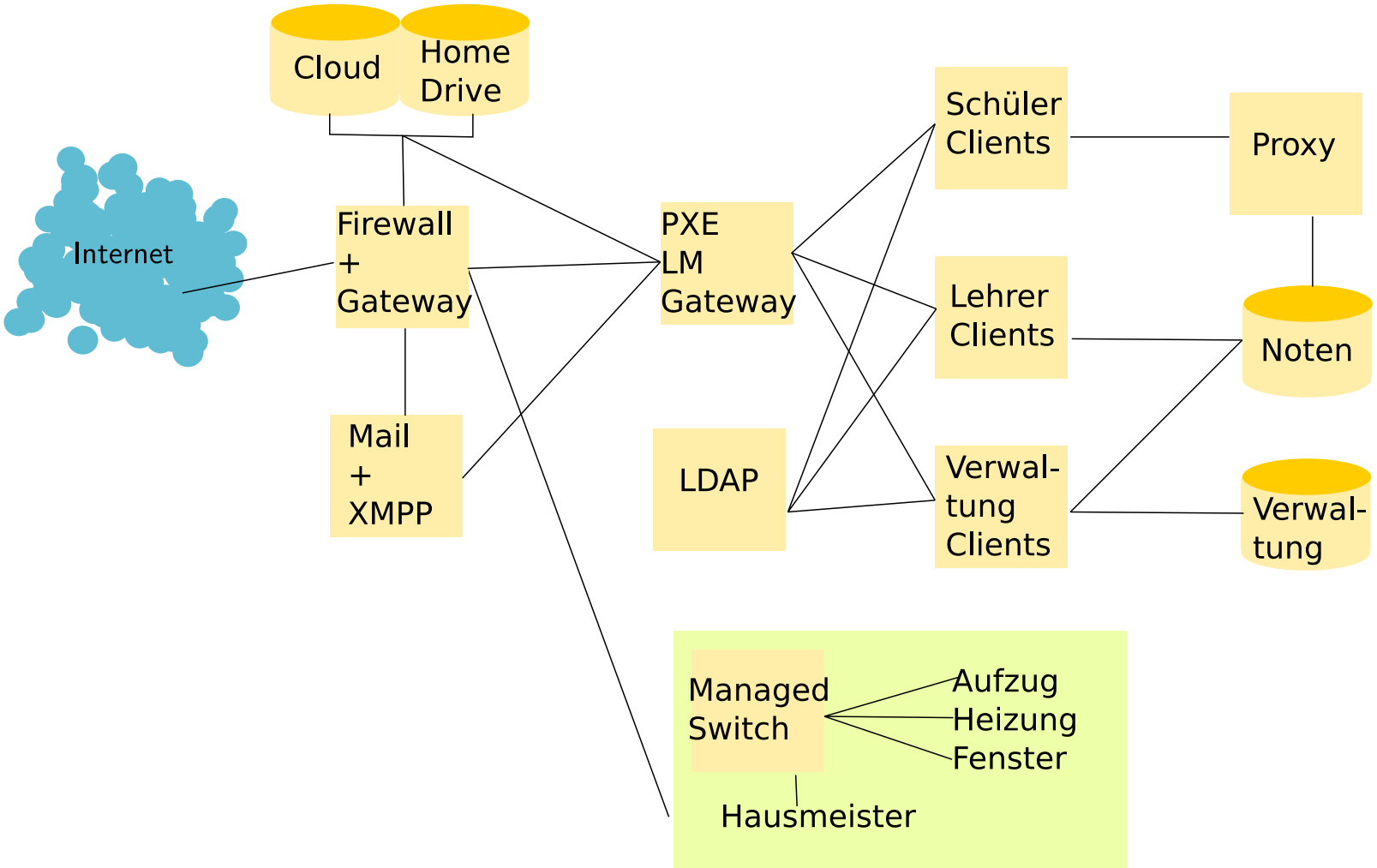
Und alles ist freie Software!

Anwendungen für Lehrer und Verwaltung (LK)

- Klassenlisten, Studenpläne(?), Zensuren, Raumplanung: Bringt Linuxmuster mit

(Webinterface für Vertretungsplan vorhanden?)

Beispiel einer Infrastruktur (PS)



Isolierte Infrastruktur

Was muss bedacht werden? (LK)

- Schüler-Arbeitsplätze: Internetzugriff erst nach Freigabe im Gateway, lesender Zugriff auf Noten-DB
- Lehrer: Zugriff auf Noten-DB, aber nicht Verwaltungs-DB
- Verwaltung: Zugriff auf Noten-DB und Verwaltungs-DB
- Embedded: Isoliert zueinander, manches muss leider ans Netz (Knebel-Support-Verträge)
  Fenster darf nicht mit Aufzug reden
  Fenster soll aber mit Heizung reden dürfen

Offline-Updates (SF)

- Nicht jede Schule hat VDSL oder FTTH
- Linuxmuster-Instanz muss lokales Repository für Clients anbieten
- Lokales Repository kann auch eigene Software bereitstellen
- Admins entscheiden (in Absprache mit Lehrern und Verwaltung), wann Upgrades ausgerollt werden

Authentifizierung: 2FA (SF)

- Passwörter sind schnell mitgelesen (Keylogger, ...)
- Passwörter sind oft unsicher (persönliches Datum, ...)

2FA: Umsetzung (SF)

- Smartcards, NFC:
  Kosten, Token kann unsicher werden (Mifare Classic). BYOD?
- GnuPG-Smartcard mit USB-Reader: ca. 20€
- Yubikeys: Unfrei, nur ein Hersteller ($\rightarrow$ abhängig), Lücken bekannt
- TOTP: (vom Smartphone generiert) fällt weg
- HOTP: nicht nutzerfreundlich (TAN-Liste neben Tastatur)
- Provider: PrivacyIdea ?

Der Zoo an Authentifizierungen (SF)

- Linux/SSH: LDAP, krb, RADIUS, Pubkey, GPG, X.509 (alles, was PAM zu bieten hat)
- Mail: LDAP, X.509, krb/GSSAPI
- Nextcloud: LDAP, X.509(?) Shibboleth?
- Moodle: LDAP?, X.509(?)Shibboleth
- WLAN (802.1X): LDAP, RADIUS, X.509
- OpenVPN: X.509, RADIUS

X.509-Zertifikat scheint am sinnvollsten (SF)

- Breite Unterstützung, auch im Webbrowser
- SC kann mit Schülerausweis/Mensakarte kombiniert werden
- Schule betreibt eigene PKI, Schulverwaltung ist RA
- Pubkeys werden im LDAP gespeichert
- auch S/MIME (E-Mail-Signierung -Verschlüsselung) möglich
- CA stellt Zertifikat für RADIUS bereit

Bleibt immer noch die Frage der Kosten...

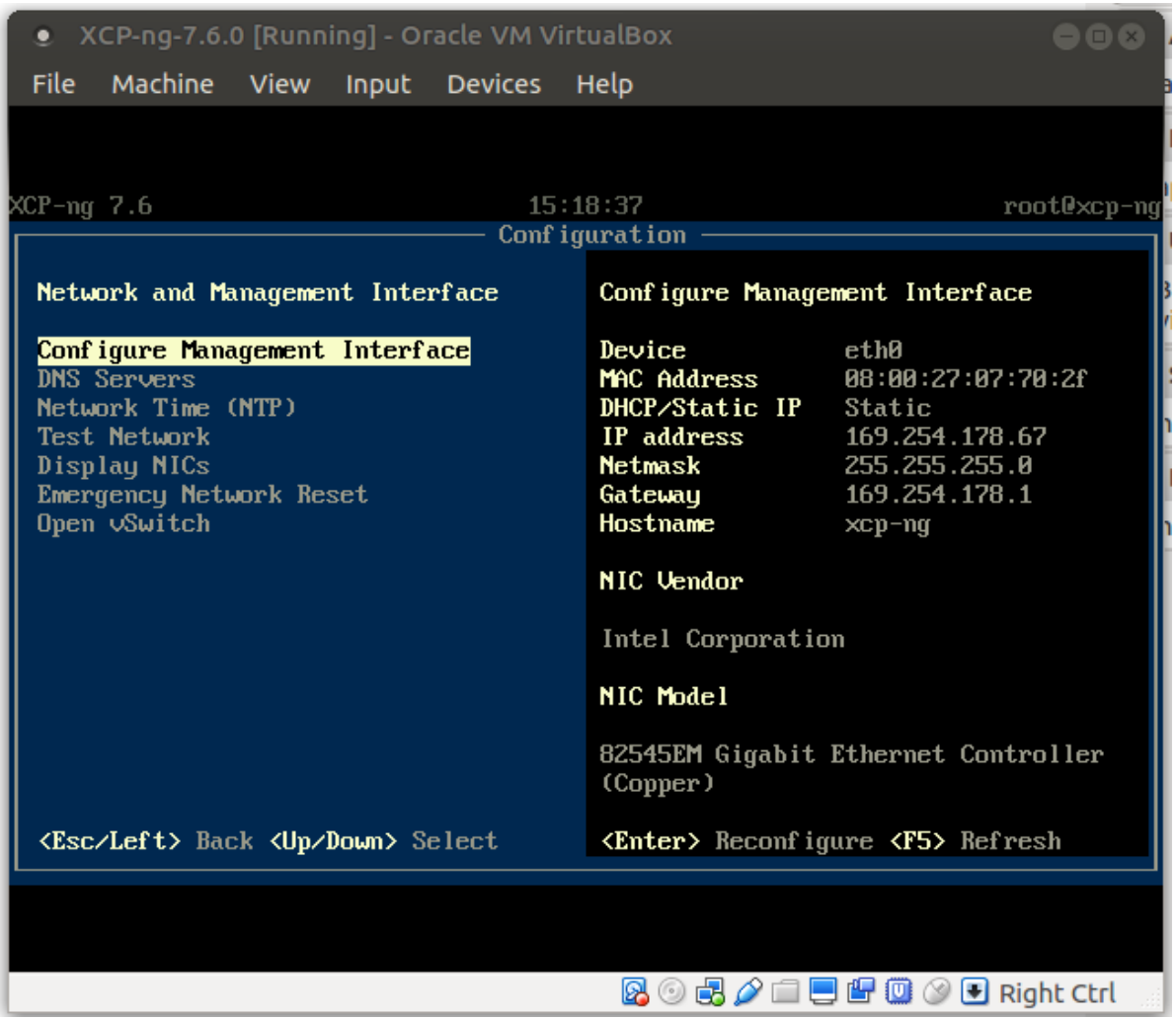
Installation Linuxmuster 6.2 (SF)

Nach Anleitung:

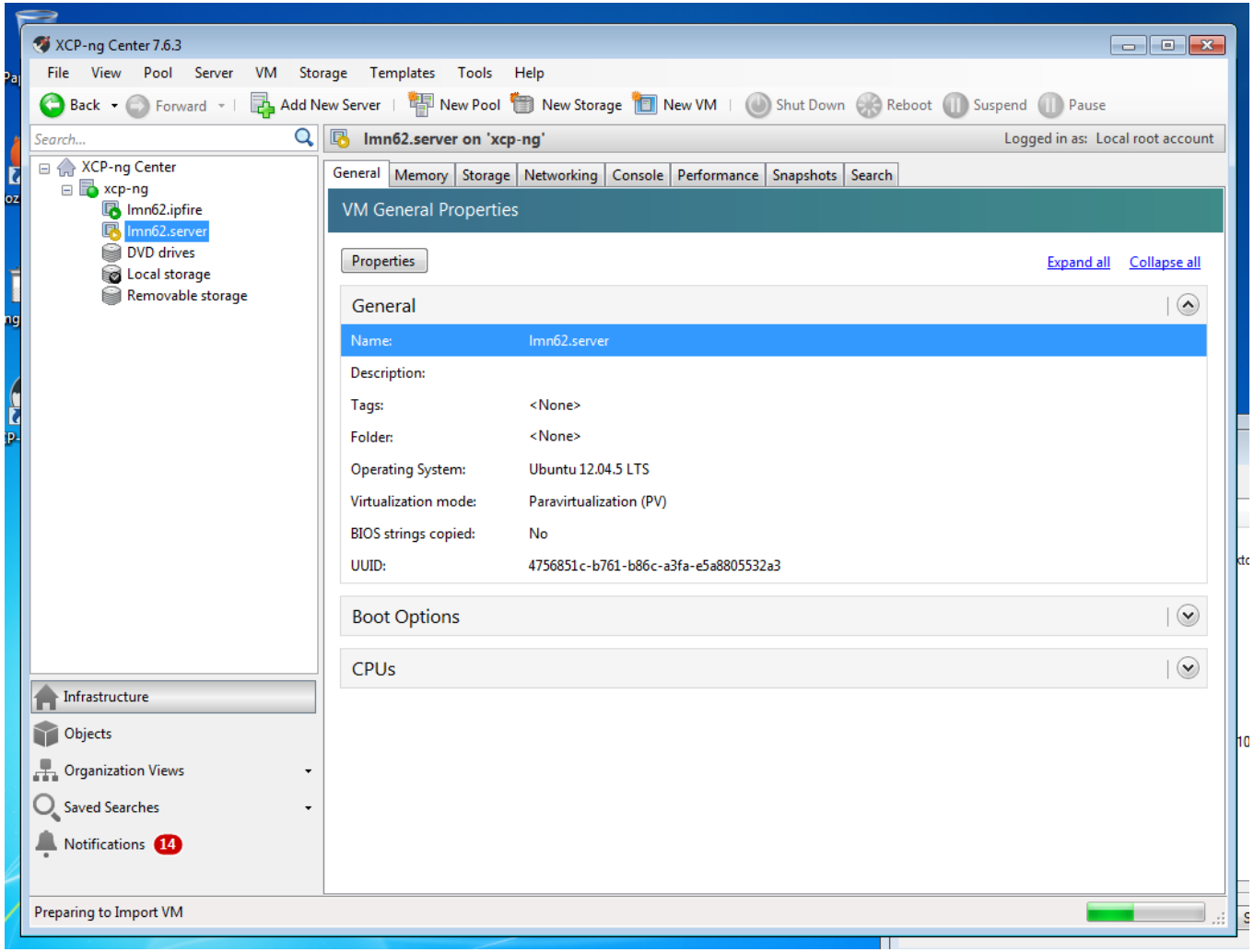
`http://docs.linuxmuster.net/de/latest/getting-started/install-on-xcp-ng/`

- Virtualisierung mit Xen (XCP-ng)
- `dom0` wird mit XCP-ng Center (Windows-Software) gesteuert
- Komponenten (als `domU`): Linuxmuster-Server, Firewall (IPFire)

dom0 (SF)


XCP-ng-7.6.0 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
XCP-ng 7.6
15:18:37
root@xcp-ng
Configuration
Network and Management Interface
Configure Management Interface
DNS Servers
Network Time (NTP)
Test Network
Display NICs
Emergency Network Reset
Open vSwitch
<Esc/Left> Back <Up/Down> Select
Configure Management Interface
Device eth0
MAC Address 08:00:27:07:70:2f
DHCP/Static IP Static
IP address 169.254.178.67
Netmask 255.255.255.0
Gateway 169.254.178.1
Hostname xcp-ng
NIC Vendor
Intel Corporation
NIC Model
82545EM Gigabit Ethernet Controller (Copper)
<Enter> Reconfigure <F5> Refresh
Right Ctrl

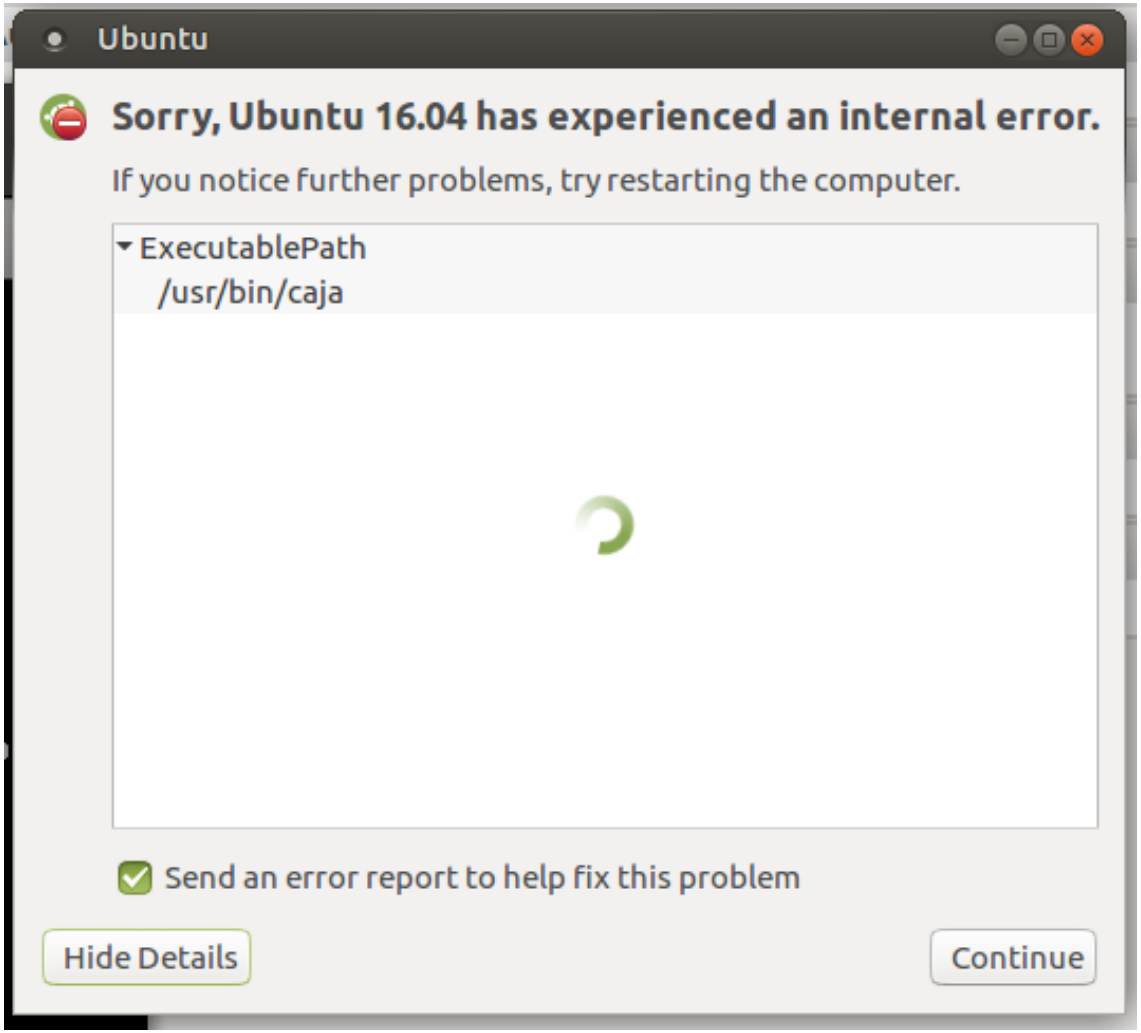
XCP-ng Center (SF)



Generelle Probleme (SF)

- Host wirft unverständliche Fehlermeldungen
- Windows-VM will plötzlich nicht mehr starten
- Xen hat Probleme mit USB-Netzwerk
  $\rightarrow$ Ubuntu-VM als Gateway
- Ubuntu-Gateway-VM hat plötzlich kaputtes ext4
- gluster auf den Hosts funktioniert irgendwie nicht
  Vorgestern war von 4 Hosts einer nutzbar
- Virtualbox hat GUI-Eigenheiten
  (z.B. NIC lässt sich während der VM-Ausführung ändern, aber erst nach Neustart tritt Änderung ein)

Grrr! (SF)


Ubuntu
Sorry, Ubuntu 16.04 has experienced an internal error.
If you notice further problems, try restarting the computer.
ExecutablePath
/usr/bin/caja
Send an error report to help fix this problem
Hide Details
Continue

Grrr! (SF)

Network Interface Cards

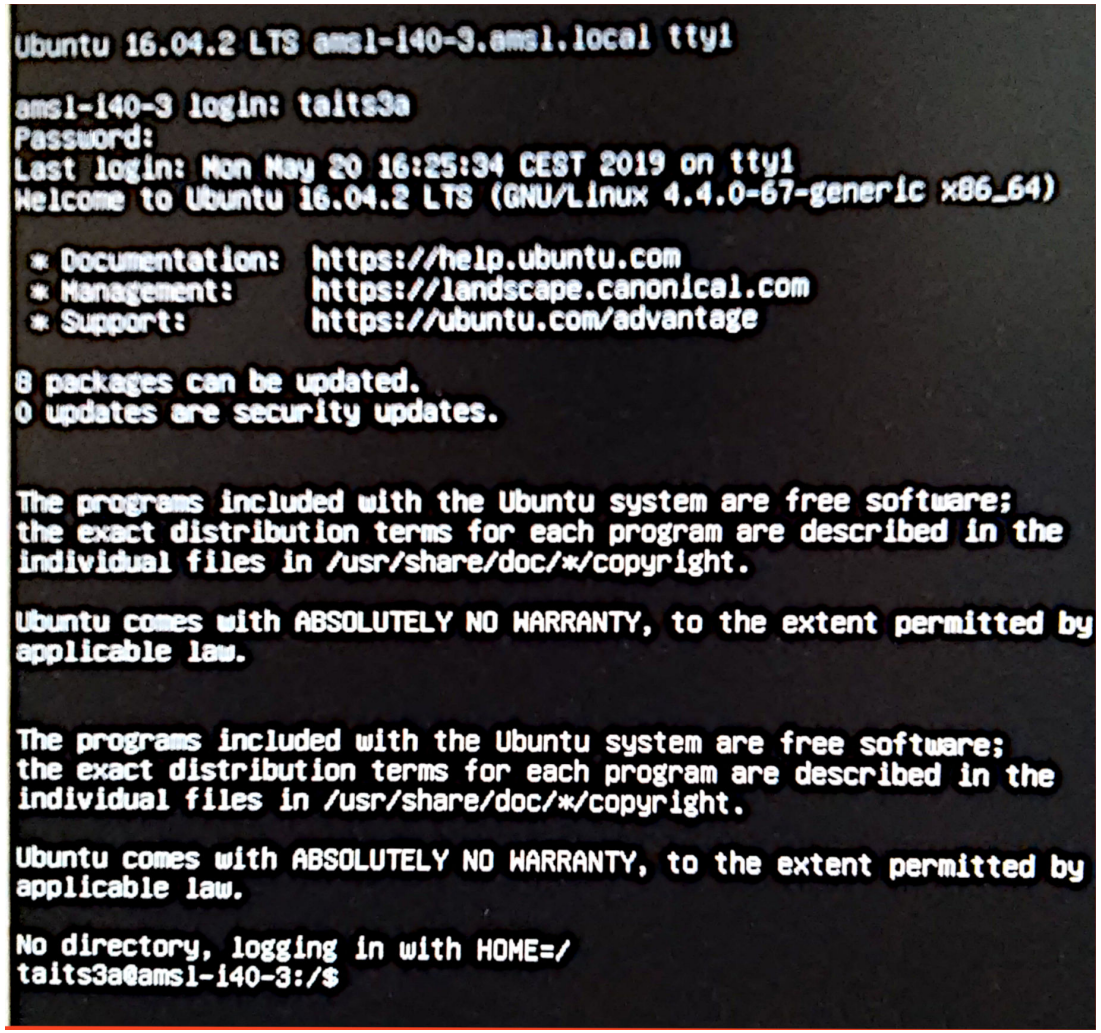
Interfaces

NIC	MAC	Link Status	Speed	Duplex	Vendor	Device
NIC 2	08:00:27:98:3d:d9	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gig...
NIC 3	08:00:27:38:4e:75	Disconnected	-	-	Intel Corporation	82545EM Gig...
NIC usb0	02:1b:1d:43:66:06	Disconnected	-	-		
NIC 0	08:00:27:07:70:2f	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gig...
NIC 1	08:00:27:8b:69:94	Connected	1000 Mbit/s	Full	Intel Corporation	82545EM Gig...

Grrr! (SF)

```
[  112.111003] EXT4-fs error (device sda1): ext4_find_entry:1309: inode #2: comm
 exe: reading directory lblock 0
[  112.111629] EXT4-fs (sda1): previous I/O error to superblock detected
mount: mounting /sys on /root/sys failed: No such file or directory
[  112.112938] EXT4-fs error (device sda1): ext4_find_entry:1309: inode #2: comm
 exe: reading directory lblock 0
[  112.113556] EXT4-fs (sda1): previous I/O error to superblock detected
mount: mounting /proc on /root/proc failed: No such file or directory
[  112.114448] EXT4-fs error (device sda1): ext4_find_entry:1309: inode #2: comm
 init: reading directory lblock 0
[  112.115094] EXT4-fs (sda1): previous I/O error to superblock detected
Target filesystem doesn't have requested /sbin/init.
[  112.115898] EXT4-fs error (device sda1): ext4_find_entry:1309: inode #2: comm
 init: reading directory lblock 0
[  112.116455] EXT4-fs (sda1): previous I/O error to superblock detected
[  112.116841] EXT4-fs error (device sda1): ext4_find_entry:1309: inode #2: comm
 init: reading directory lblock 0
[  112.117439] EXT4-fs (sda1): previous I/O error to superblock detected
No init found. Try passing init= bootarg.


BusyBox v1.18.5 (Ubuntu 1:1.18.5-1ubuntu4.1) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs) _
```

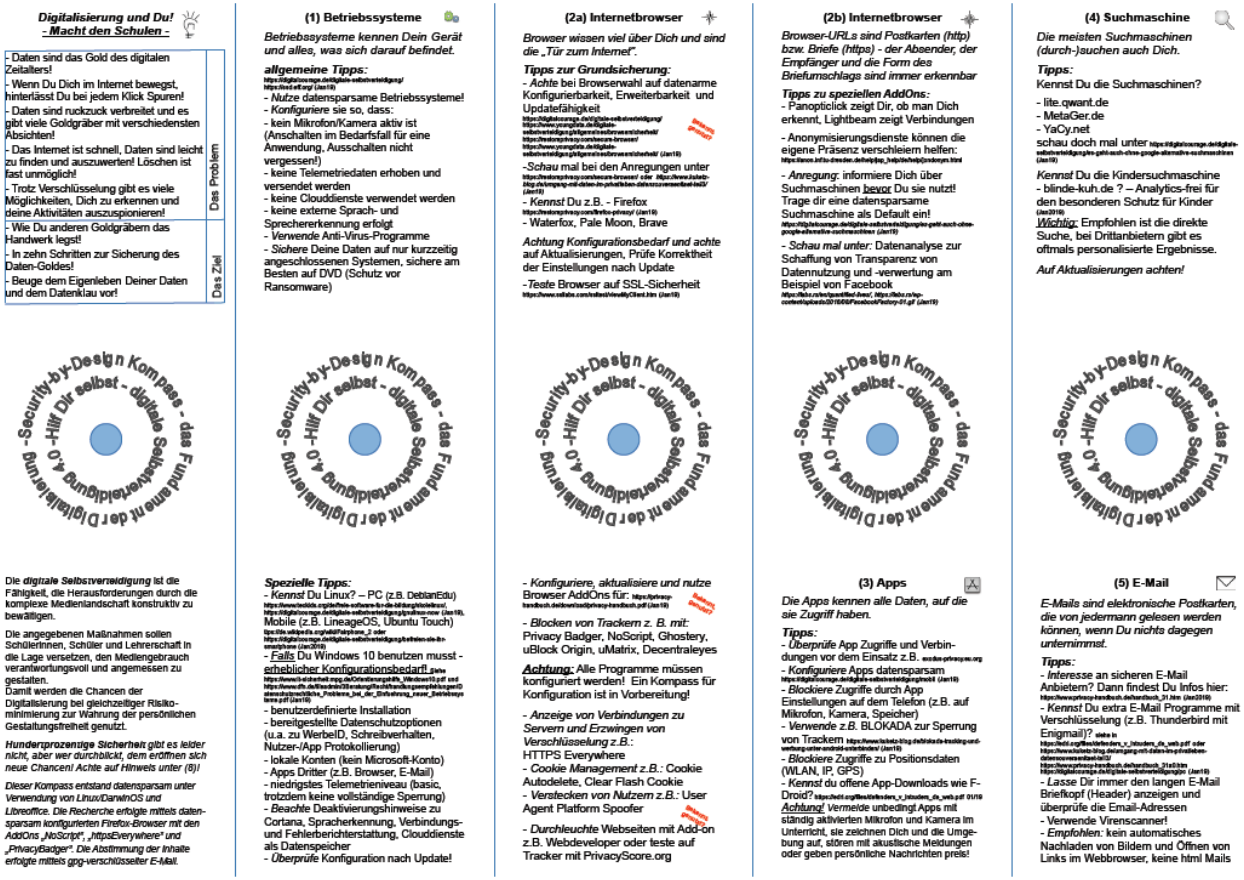
Grrr! (SF)


Ubuntu 16.04.2 LTS amsl-i40-3.amsl.local tty1
amsl-i40-3 login: taits3a
Password:
Last login: Mon May 20 16:25:34 CEST 2019 on tty1
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-67-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
8 packages can be updated.
0 updates are security updates.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
No directory, logging in with HOME=/
taits3a@amsl-i40-3:/$

Probleme bei der Installation (SF)

- In `/etc/network/interfaces`: `:%s/eth0/eth3/g` (Nachschauen mit `ip link`)
- GPG-Key für `pkg.linuxmuster.net` musste manuell hinzugefügt werden
- `linuxmuster-setup -first` überschreibt `resolv.conf` →DNS tut während der Ausführung nicht mehr
- LDAP-Schema `sophomorix` fehlt
  In welchem Paket ist es enthalten?

Digital-Kompass (LK)



Digitalisierung und Du!
- Macht den Schulen -

Das Problem
- Daten sind das Gold des digitalen Zeitalters!
- Wenn Du Dich im Internet bewegst, hinterlässt Du bei jedem Klick Spuren!
- Daten sind ruckzuck verbreitet und es gibt viele Goldgräber mit verschiedensten Absichten!
- Das Internet ist schnell, Daten sind leicht zu finden und auszuwerten! Löschen ist fast unmöglich!
- Trotz Verschlüsselung gibt es viele Möglichkeiten, Dich zu erkennen und deine Aktivitäten auszuspionieren!
- Wie Du anderen Goldgräbern das Handwerk legst!

Das Ziel
- In zehn Schritten zur Sicherung des Daten-Goldes!
- Beuge dem Eigenleben Deiner Daten und dem Datenklau vor!

Security-by-Design Kompass - Hilf Dir selbst - digitale Selbstverteidigung 4.0 - das Fun- und ame nt der Digitalbeleuchtung

Die *digitale Selbstverteidigung* ist die Fähigkeit, die Herausforderungen durch die komplexe Medienlandschaft konstruktiv zu bewältigen.

Die angegebenen Maßnahmen sollen Schülerinnen, Schüler und Lehrerschaft in die Lage versetzen, den Mediengebrauch verantwortungsvoll und angemessen zu gestalten.
Damit werden die Chancen der Digitalisierung bei gleichzeitiger Risiko-minimierung zur Wahrung der persönlichen Gestaltungsfreiheit genutzt.

***Hundertprozentige Sicherheit** gibt es leider nicht, aber wer durchblickt, dem eröffnen sich neue Chancen! Achte auf Hinweis unter (B)!*

Dieser Kompass entstand datensparsam unter Verwendung von Linux/DarwinOS und Libreoffice. Die Recherche erfolgte mittels daten-sparsam konfigurierten Firefox-Browser mit den AddOns „NoScript", „HttpsEverywhere" und „PrivacyBadger". Die Abstimmung der Inhalte erfolgte mittels gpg-verschlüsselter E-Mail.

(1) Betriebssysteme

Betriebssysteme kennen Dein Gerät und alles, was sich darauf befindet.

allgemeine Tipps:
- *Nutze* datensparsame Betriebssysteme!
- *Konfiguriere* sie so, dass:
- kein Mikrofon/Kamera aktiv ist (Anschalten im Bedarfsfall für eine Anwendung, Ausschalten nicht vergessen!)
- keine Telemetriedaten erhoben und versendet werden
- keine Clouddienste verwendet werden
- keine externe Sprach- und Sprechererkennung erfolgt
- *Verwende* Anti-Virus-Programme
- *Sichere* Deine Daten auf nur kurzzeitig angeschlossenen Systemen, sichere am Besten auf DVD (Schutz vor Ransomware)

Spezielle Tipps:
- *Kennst* Du Linux? – PC (z.B. DebianEdu)
Mobile (z.B. LineageOS, Ubuntu Touch)
- *Falls* Du Windows 10 benutzen musst - erheblicher Konfigurationsbedarf!
- benutzerdefinierte Installation
- bereitgestellte Datenschutzoptionen (u.a. zu WerbeID, Schreibverhalten, Nutzer-/App Protokollierung)
- lokale Konten (kein Microsoft-Konto)
- Apps Dritter (z.B. Browser, E-Mail)
- niedrigstes Telemetrieniveau (basic, trotzdem keine vollständige Sperrung)
- *Beachte* Deaktivierungshinweise zu Cortana, Spracherkennung, Verbindungs- und Fehlerberichterstattung, Clouddienste als Datenspeicher
- *Überprüfe* Konfiguration nach Update!

(2a) Internetbrowser

Browser wissen viel über Dich und sind die „Tür zum Internet".

Tipps zur Grundsicherung:
- *Achte* bei Browserwahl auf datenarme Konfigurierbarkeit, Erweiterbarkeit und Updatefähigkeit
- *Schau* mal bei den Anregungen unter
- *Kennst* Du z.B. - Firefox
- Waterfox, Pale Moon, Brave

Achtung Konfigurationsbedarf und achte auf Aktualisierungen, Prüfe Korrektheit der Einstellungen nach Update

- *Teste* Browser auf SSL-Sicherheit

- *Konfiguriere, aktualisiere und nutze* Browser AddOns für:
- *Blocken von Trackern z. B. mit:* Privacy Badger, NoScript, Ghostery, uBlock Origin, uMatrix, Decentraleyes

Achtung: Alle Programme müssen konfiguriert werden! Ein Kompass für Konfiguration ist in Vorbereitung!

- *Anzeige von Verbindungen zu Servern und Erzwingen von Verschlüsselung z.B.:* HTTPS Everywhere
- *Cookie Management z.B.:* Cookie Autodelete, Clear Flash Cookie
- *Verstecken von Nutzern z.B.:* User Agent Platform Spoofer

- *Durchleuchte* Webseiten mit Add-on z.B. Webdeveloper oder teste auf Tracker mit PrivacyScore.org

(2b) Internetbrowser

Browser-URLs sind Postkarten (http) bzw. Briefe (https) - der Absender, der Empfänger und die Form des Briefumschlags sind immer erkennbar

Tipps zu speziellen AddOns:
- Panopticlick zeigt Dir, ob man Dich erkennt, Lightbeam zeigt Verbindungen

- Anonymisierungsdienste können die eigene Präsenz verschleiern helfen:

- *Anregung:* informiere Dich über Suchmaschinen *bevor* Du sie nutzt! Trage dir eine datensparsame Suchmaschine als Default ein!

- *Schau mal unter:* Datenanalyse zur Schaffung von Transparenz von Datennutzung und -verwertung am Beispiel von Facebook

(3) Apps

Die Apps kennen alle Daten, auf die sie Zugriff haben.

Tipps:
- *Überprüfe* App Zugriffe und Verbindungen vor dem Einsatz z.B.
- *Konfiguriere* Apps datensparsam
- *Blockiere* Zugriffe durch App Einstellungen auf dem Telefon (z.B. auf Mikrofon, Kamera, Speicher)
- *Verwende z.B.* BLOKADA zur Sperrung von Trackern
- *Blockiere* Zugriffe zu Positionsdaten (WLAN, IP, GPS)
- *Kennst* du offene App-Downloads wie F-Droid?

Achtung! *Vermeide* unbedingt Apps mit ständig aktivierten Mikrofon und Kamera im Unterricht, sie zeichnen Dich und die Umgebung auf, stören mit akustische Meldungen oder geben persönliche Nachrichten preis!

(4) Suchmaschine

Die meisten Suchmaschinen (durch-)suchen auch Dich.

Tipps:
Kennst Du die Suchmaschinen?
- lite.qwant.de
- MetaGer.de
- YaCy.net
schau doch mal unter

Kennst Du die Kindersuchmaschine
- blinde-kuh.de ? – Analytics-frei für den besonderen Schutz für Kinder

Wichtig: Empfohlen ist die direkte Suche, bei Drittanbietern gibt es oftmals personalisierte Ergebnisse.

Auf Aktualisierungen achten!

(5) E-Mail

E-Mails sind elektronische Postkarten, die von jedermann gelesen werden können, wenn Du nichts dagegen unternimmst.

Tipps:
- *Interesse* an sicheren E-Mail Anbietern? Dann findest Du Infos hier:
- *Kennst* Du extra E-Mail Programme mit Verschlüsselung (z.B. Thunderbird mit Enigmail)?
- *Lasse* Dir immer den langen E-Mail Briefkopf (Header) anzeigen und überprüfe die Email-Adressen
- Verwende Virenscanner!
- *Empfohlen:* kein automatisches Nachladen von Bildern und Öffnen von Links im Webbrowser, keine html Mails

Abbildung: aus `https://omen.cs.ovgu.de/itiams/deutsch/secbydesign/index.html`

Digital-Kompass (LK)

Abbildung: aus `https://omen.cs.ovgu.de/itiams/deutsch/secbydesign/index.html`

Digital-Kompass (LK)

(1) Betriebssysteme

Betriebssysteme kennen Dein Gerät und alles, was sich darauf befindet.

allgemeine Tipps:
https://digitalcourage.de/digitale-selbstverteidigung/
https://ssd.eff.org/ (Jan19)
- *Nutze* datensparsame Betriebssysteme!
- *Konfiguriere* sie so, dass:
- kein Mikrofon/Kamera aktiv ist (Anschalten im Bedarfsfall für eine Anwendung, Ausschalten nicht vergessen!)
- keine Telemetriedaten erhoben und versendet werden
- keine Clouddienste verwendet werden
- keine externe Sprach- und Sprechererkennung erfolgt
- *Verwende* Anti-Virus-Programme
- *Sichere* Deine Daten auf nur kurzzeitig angeschlossenen Systemen, sichere am Besten auf DVD (Schutz vor Ransomware)

(2a) Internetbrowser

Browser wissen viel über Dich und sind die „Tür zum Internet".

Tipps zur Grundsicherung:
- *Achte* bei Browserwahl auf datenarme Konfigurierbarkeit, Erweiterbarkeit und Updatefähigkeit
https://digitalcourage.de/digitale-selbstverteidigung/
https://www.youngdata.de/digitale-selbstverteidigung/allgemeines/browsersicherheit/
https://restoreprivacy.com/secure-browser/
https://www.youngdata.de/digitale-selbstverteidigung/allgemeines/browsersicherheit/ (Jan19)

Bekannt, genutzt?

-*Schau* mal bei den Anregungen unter
https://restoreprivacy.com/secure-browser/ oder *https://www.kuketz-blog.de/umgang-mit-daten-im-privatleben-datensouveraenitaet-teil3/ (Jan19)*
- *Kennst* Du z.B. - Firefox
https://restoreprivacy.com/firefox-privacy/ (Jan19)
- Waterfox, Pale Moon, Brave

Achtung Konfigurationsbedarf und achte auf Aktualisierungen, Prüfe Korrektheit der Einstellungen nach Update

-*Teste* Browser auf SSL-Sicherheit
https://www.ssllabs.com/ssltest/viewMyClient.htm (Jan19)

Abbildung: aus SiSy 2019, Prof.Dr-Ing. Jana Dittmann, Mario Hildebrand

Digital-Kompass (LK)

nd sind

arme
und

Bekannt, ge nutzt?

nter
kuketz-
t-teil3/

l achte
theit

eit

(2b) Internetbrowser

Browser-URLs sind Postkarten (http) bzw. Briefe (https) - der Absender, der Empfänger und die Form des Briefumschlags sind immer erkennbar

Tipps zu speziellen AddOns:
- Panopticlick zeigt Dir, ob man Dich erkennt, Lightbeam zeigt Verbindungen

- Anonymisierungsdienste können die eigene Präsenz verschleiern helfen: https://anon.inf.tu-dresden.de/help/jap_help/de/help/jondonym.html

- *Anregung*: informiere Dich über Suchmaschinen bevor Du sie nutzt! Trage dir eine datensparsame Suchmaschine als Default ein! https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen (Jan19)

- *Schau mal unter*: Datenanalyse zur Schaffung von Transparenz von Datennutzung und -verwertung am Beispiel von Facebook https://labs.rs/en/quantified-lives/, https://labs.rs/wp-content/uploads/2016/08/FacebookFactory-01.gif (Jan19)

(4) Suchmaschine

Die meisten Suchmaschinen (durch-)suchen auch Dich.

Tipps:
Kennst Du die Suchmaschinen?

- lite.qwant.de
- MetaGer.de
- YaCy.net

schau doch mal unter https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen (Jan19)

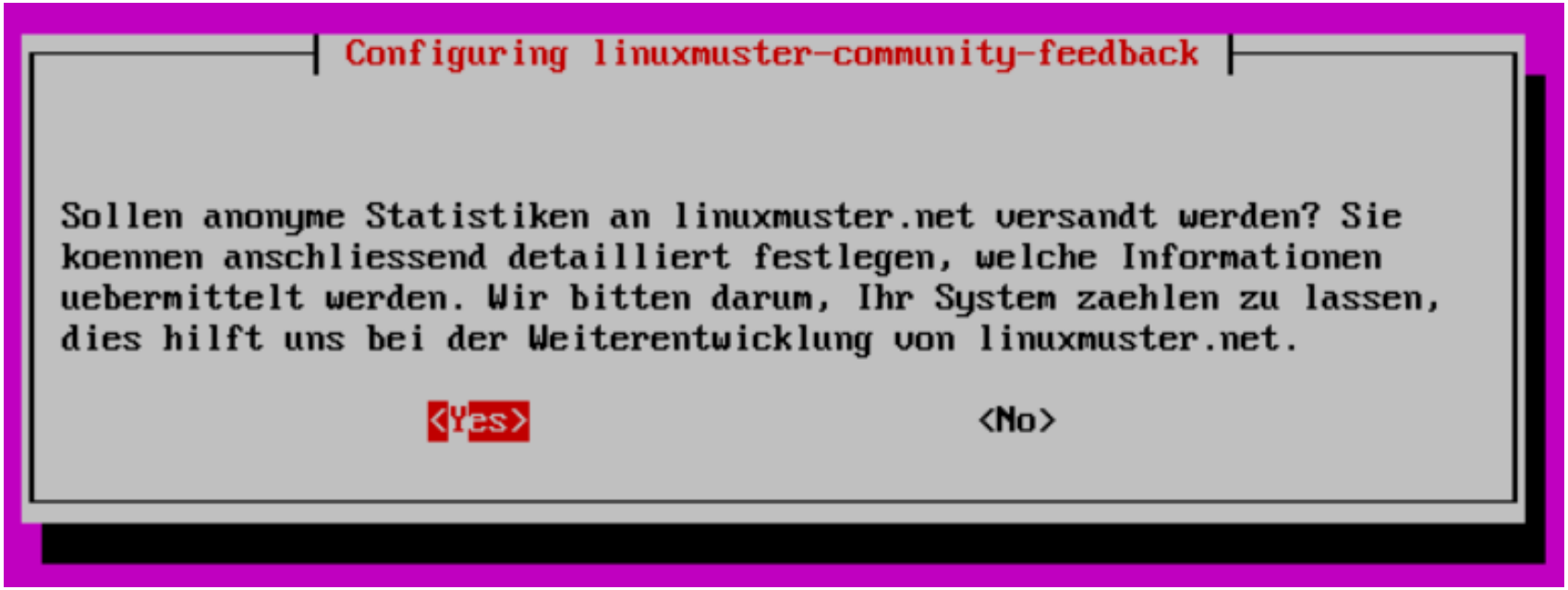
Kennst Du die Kindersuchmaschine - blinde-kuh.de ? – Analytics-frei für den besonderen Schutz für Kinder (Jan2019)

Wichtig: Empfohlen ist die direkte Suche, bei Drittanbietern gibt es oftmals personalisierte Ergebnisse.

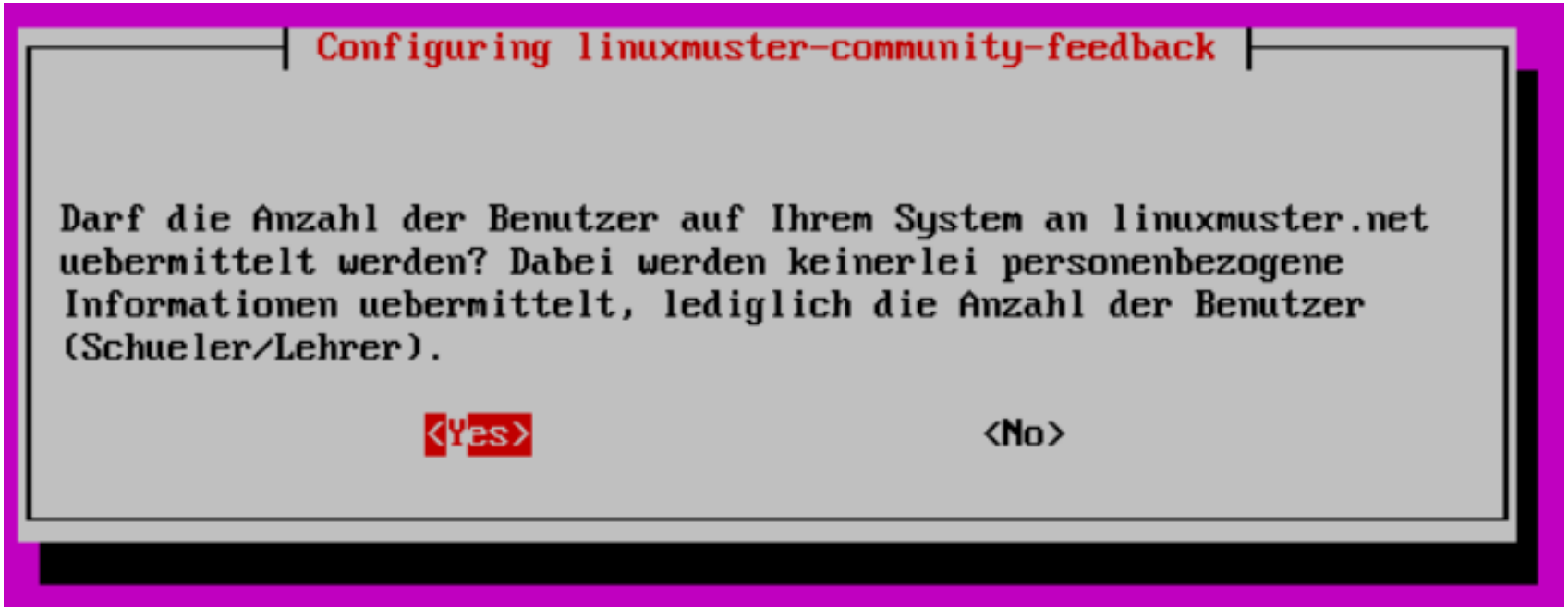
Auf Aktualisierungen achten!

Abbildung: aus SiSy 2019, Prof.Dr-Ing. Jana Dittmann, Mario Hildebrand

Im Setup (SF)


Configuring linuxmuster-community-feedback
Sollen anonyme Statistiken an linuxmuster.net versandt werden? Sie koennen anschliessend detailliert festlegen, welche Informationen uebermittelt werden. Wir bitten darum, Ihr System zaehlen zu lassen, dies hilft uns bei der Weiterentwicklung von linuxmuster.net.
<Yes>
<No>

Im Setup (SF)


Configuring linuxmuster-community-feedback
Darf die Anzahl der Benutzer auf Ihrem System an linuxmuster.net uebermittelt werden? Dabei werden keinerlei personenbezogene Informationen uebermittelt, lediglich die Anzahl der Benutzer (Schueler/Lehrer).
<Yes>
<No>

Fragen an unseren Gast (SF)

- Machen wir was falsch? Ist LM 6.2 zu alt?
- Warum ein altes Ubuntu? (12.04)
- Warum ist das Xen-Image halbgar?
  (Image ist riesig, trotzdem müssen viele Pakete aufwendig nachinstalliert werden)
- Warum verlangt die Installation einen Internetzugang?
  Was ist mit Schulen, die offline sind?

Installation LM 6.2 Server (SF)

- Lief, wie in Doku beschrieben, durch
- Naja, nicht ganz:
  - `apache2` startet nicht (→ Schulkonsole)
  - `slapd` startet auch nicht
  - `cupsd` auch nicht (erst mal egal)
- `domUs` bekamen mehr Speicher

Probleme bei der Installation (SF)

- LM 6.2 Repository: (im Forum versteckt)
  `:%s/pkg.linuxmuster.net/archive.linuxmuster.net`
- `slapd`: Probleme mit TLS-Zertifikat
- `cloop`-Server (stellt Images bereit):
  Repository `cloop.linuxmuster.net` wurde abgeschaltet
  https://ask.linuxmuster.net/... half

nmap RED interface (SF)

```
senf@billiejoe:~/Nextcloud/OvGU/TAITS/Referat_Slides$ nmap 10.42.0.0/24
#Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-26 15:53 CEST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 1.27% done; ETC: 15:53 (0:00:00 remaining)
Nmap scan report for 10.42.0.1
Host is up (0.00018s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 256 IP addresses (1 host up) scanned in 3.11 seconds
```

nmap GREEN interface (SF)

```
Starting Nmap 7.01 ( https://nmap.org ) at 2019-06-26 16:55 CEST
Nmap scan report for server.linuxmuster-net.lokal (10.16.1.1)
Host is up (0.00055s latency).
Not shown: 955 filtered ports, 32 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
113/tcp  open  ident
139/tcp  open  netbios-ssn
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
636/tcp  open  ldapssl
873/tcp  open  rsync
993/tcp  open  imaps
MAC Address: 72:7B:36:52:A9:91 (Unknown)
```

nmap GREEN interface (SF)

```
Starting Nmap 7.01 ( https://nmap.org ) at 2019-06-26 16:55 CEST
Nmap scan report for 10.16.1.4
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
MAC Address: DE:C2:DF:B9:18:44 (Unknown)
```

nmap GREEN interface (SF)

```
Starting Nmap 7.01 ( https://nmap.org ) at 2019-06-26 16:55 CEST
Nmap scan report for ipfire.linuxmuster-net.local (10.16.1.254)
Host is up (0.00056s latency).
Not shown: 993 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
81/tcp   open  hosts2-ns
222/tcp  open  rsh-spx
444/tcp  open  snpp
800/tcp  open  mdbs_daemon
801/tcp  open  device
MAC Address: 32:B0:D0:F2:BF:15 (Unknown)
```

XOA (SF)

Xen Orchestra

- Home
- Dashboard
- Self service
- Backup
- Backup NG
- XOA ?
- Settings
- Jobs
- About
- Tasks 1
- XOSAN
- New
- No support
- Sign out

xcp-ng-linuxmuster > xcp-ng-linuxmuster

lmn62.ipfire

108e6fe7-ed97-1740-755c-b853e3f1afe9

Click to edit

General | Stats | Console | Network | Disks | Snapshots | Logs | Advanced

Select disk(s)... | Copy | Ctrl+Alt+Del

```
Bringing up the red0 interface...
Starting dhcpcd on the red0 interface...                    [  OK  ]
          DHCP Assigned Settings for red0:
          IP Address:       169.254.182.80
          Hostname:         ipfire
          Subnet Mask:      255.255.0.0
          Default Gateway:
          DNS Server:
Adding static routes...                                     [  OK  ]
Starting the Cyrus SASL Server...                           [  OK  ]
Initializing kernel random number generator...              [  OK  ]
Setting time on boot...
Waiting for red connection..........................  ERROR! Not onli[ WARN ]
Starting ntpd...                                            [  OK  ]
Loading Sensor Modules: coretemp                            [  OK  ]
Starting Collection daemon...                               [  OK  ]
Starting SSH Server...                                      [  OK  ]
Starting Apache daemon...                                   [  OK  ]
Starting fcron...                                           [  OK  ]

IPFire v2.19 - www.ipfire.org
=============================
ipfire running on Linux 3.14.65-ipfire-pae i686
ipfire login:
```

slapd (SF)

```
 * Starting OpenLDAP slapd          * Starting OpenLDAP slapd
                                                                [[failf
ail]
```

```
09:12/1 server ~ # tail -n 1000 /var/log/syslog | grep slapd
Jun 12 09:01:17 server slapd[1481]: @(#) $OpenLDAP: slapd  (Sep 15 2015 18:19:06
) $#012#011buildd@lgw01-02:/build/openldap-5NvlxW/openldap-2.4.28/debian/build/s
ervers/slapd
Jun 12 09:06:46 server slapd[2821]: @(#) $OpenLDAP: slapd  (Sep 15 2015 18:19:06
) $#012#011buildd@lgw01-02:/build/openldap-5NvlxW/openldap-2.4.28/debian/build/s
ervers/slapd
Jun 12 09:12:25 server slapd[3489]: @(#) $OpenLDAP: slapd  (Sep 15 2015 18:19:06
) $#012#011buildd@lgw01-02:/build/openldap-5NvlxW/openldap-2.4.28/debian/build/s
ervers/slapd
Jun 12 09:12:25 server slapd[3489]: main: TLS init def ctx failed: -49
Jun 12 09:12:25 server slapd[3489]: slapd stopped.
Jun 12 09:12:25 server slapd[3489]: connections_destroy: nothing to destroy.
```

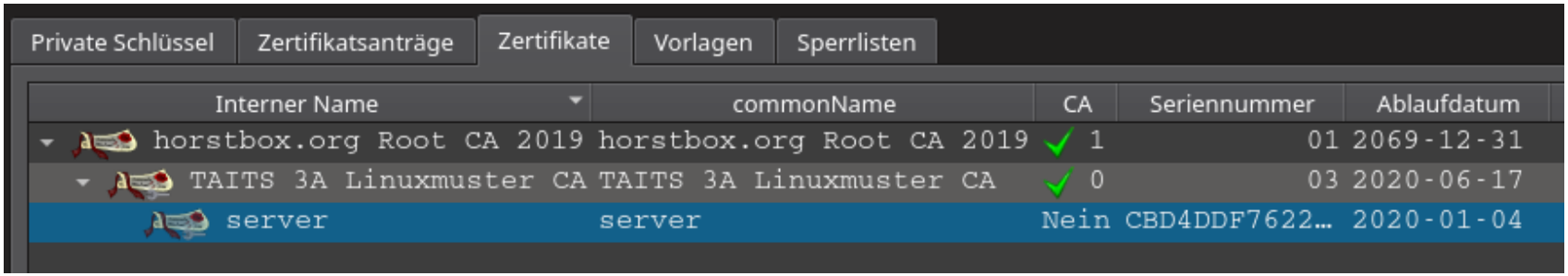
Den Pubkey dürft ihr dann finden (SF)

```
# TLS:
#TLSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCACertificateFile /etc/ssl/private/server.pem
TLSCertificateFile /etc/ssl/private/server.pem
TLSCertificateKeyFile /etc/ssl/private/server.pem
```

```
cat /etc/ssl/private/server.pem

---BEGIN RSA PRIVATE KEY---

                              ...

---END RSA PRIVATE KEY---
```

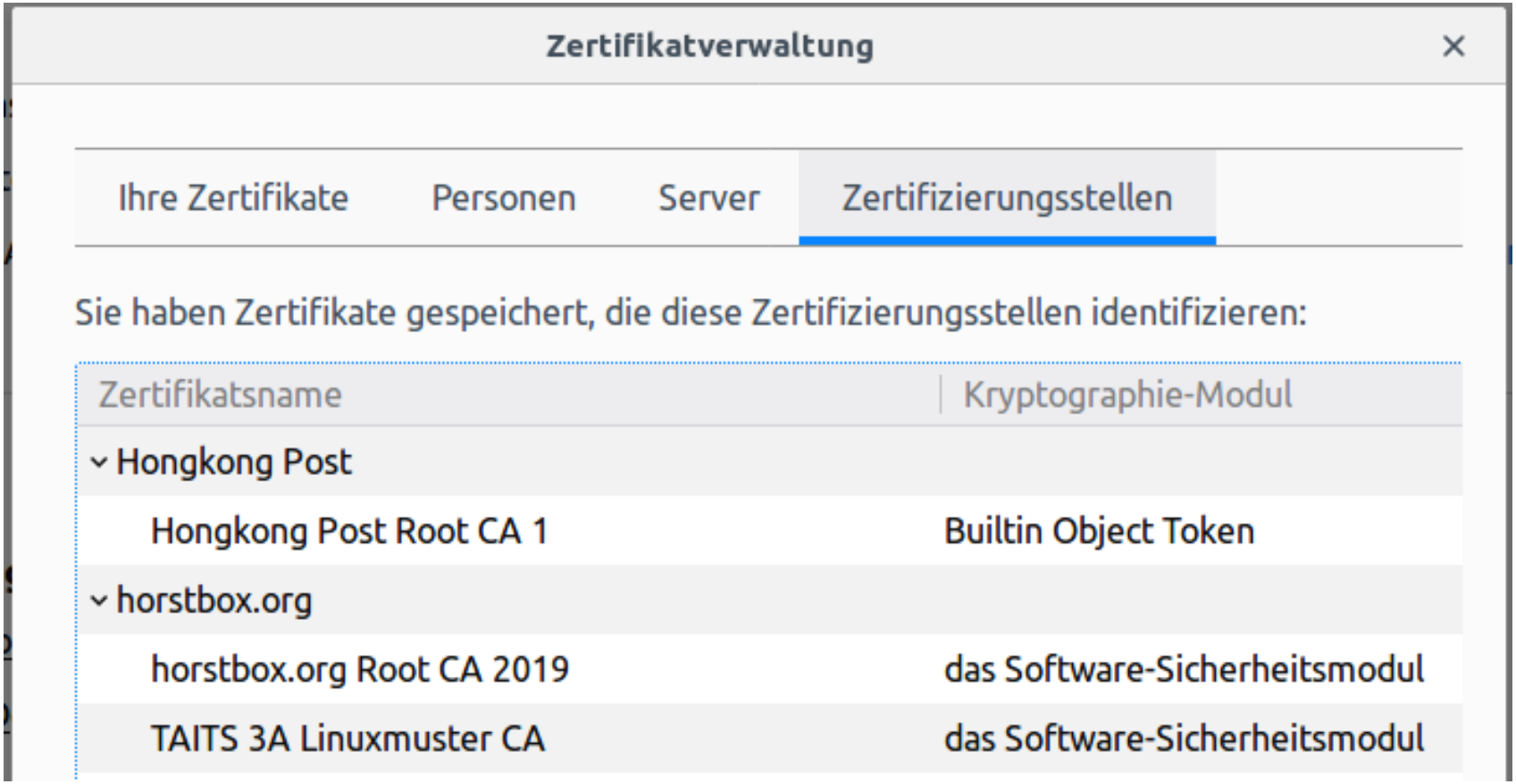
EOF

PKI aufsetzen (SF)



- Provisorische CA erstellt
- Crt für Server: apache2, slapd, RADIUS, ...
- Auch für spätere Nutzerzertifikate verwendbar (→ 2FA)
- Nutzerzertifikate dann auch für S/MIME nutzbar (unterstützen TB oder claws-mail ootb)

Firefox: CA importieren (SF)



LINBO (SF)

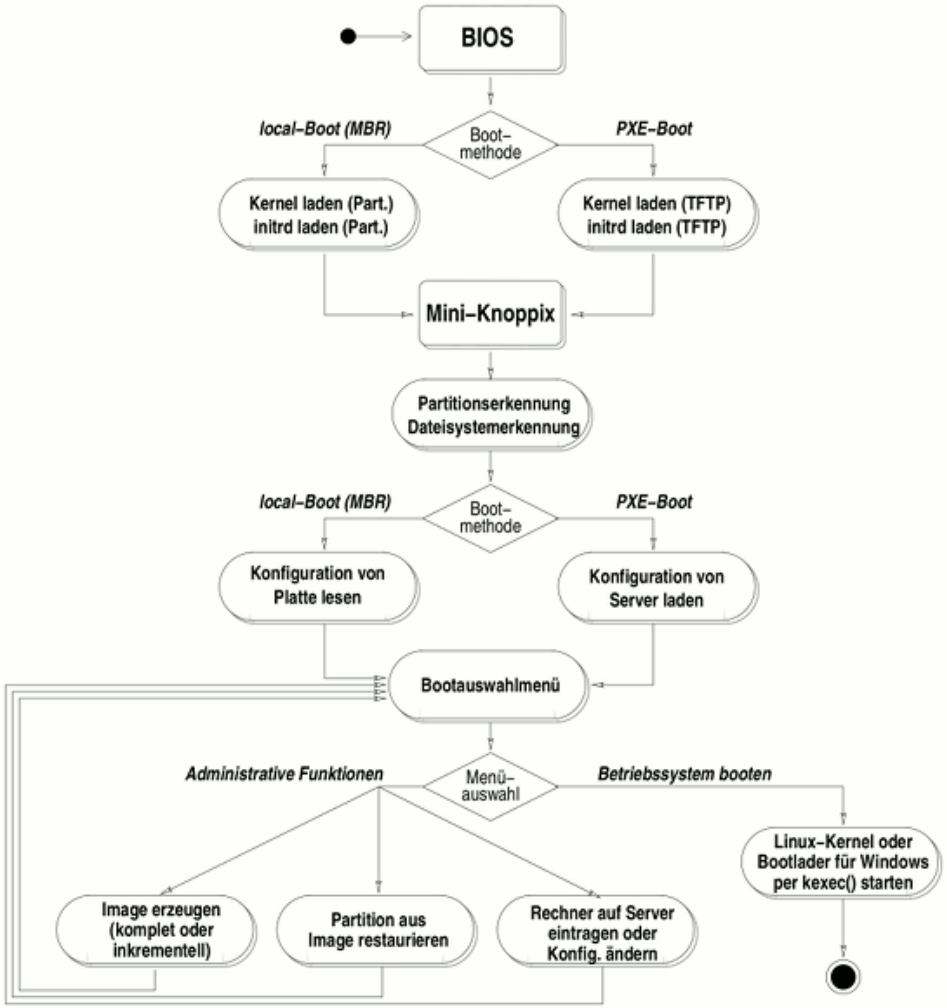
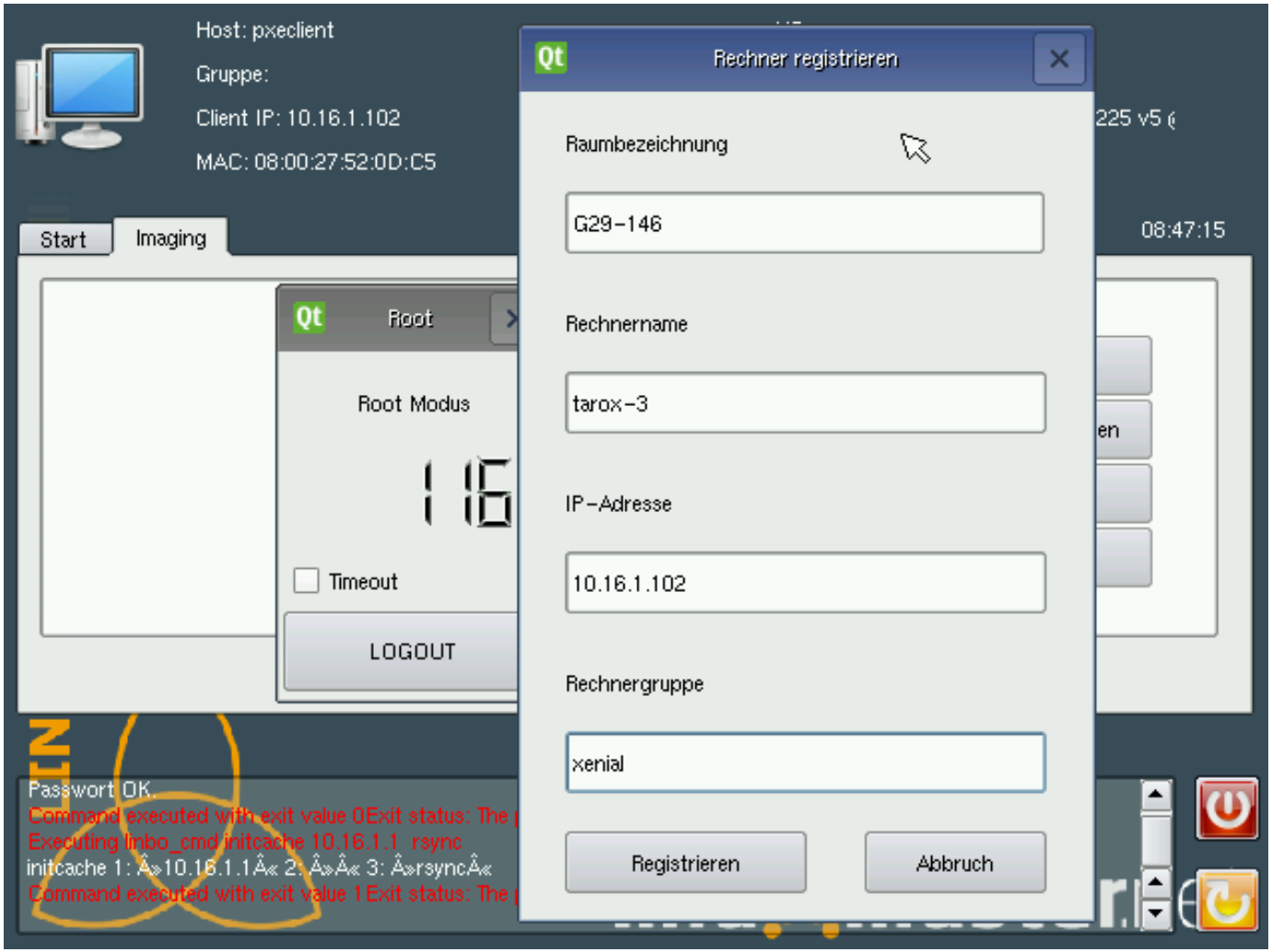


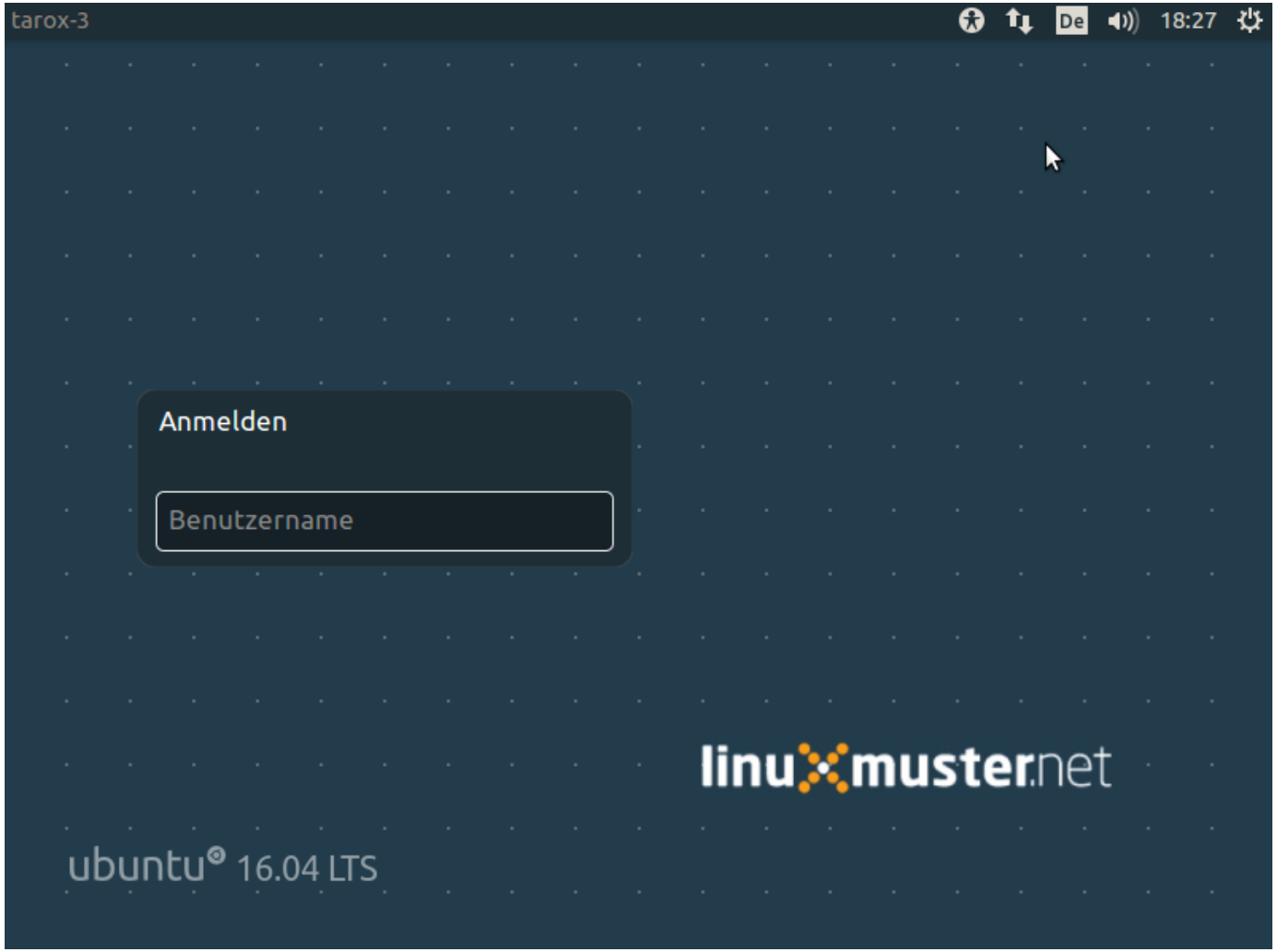
Abbildung: `http://www.knopper.net/pics/linbo-booting.gif`

Linbo: Rechner registrieren (SF)

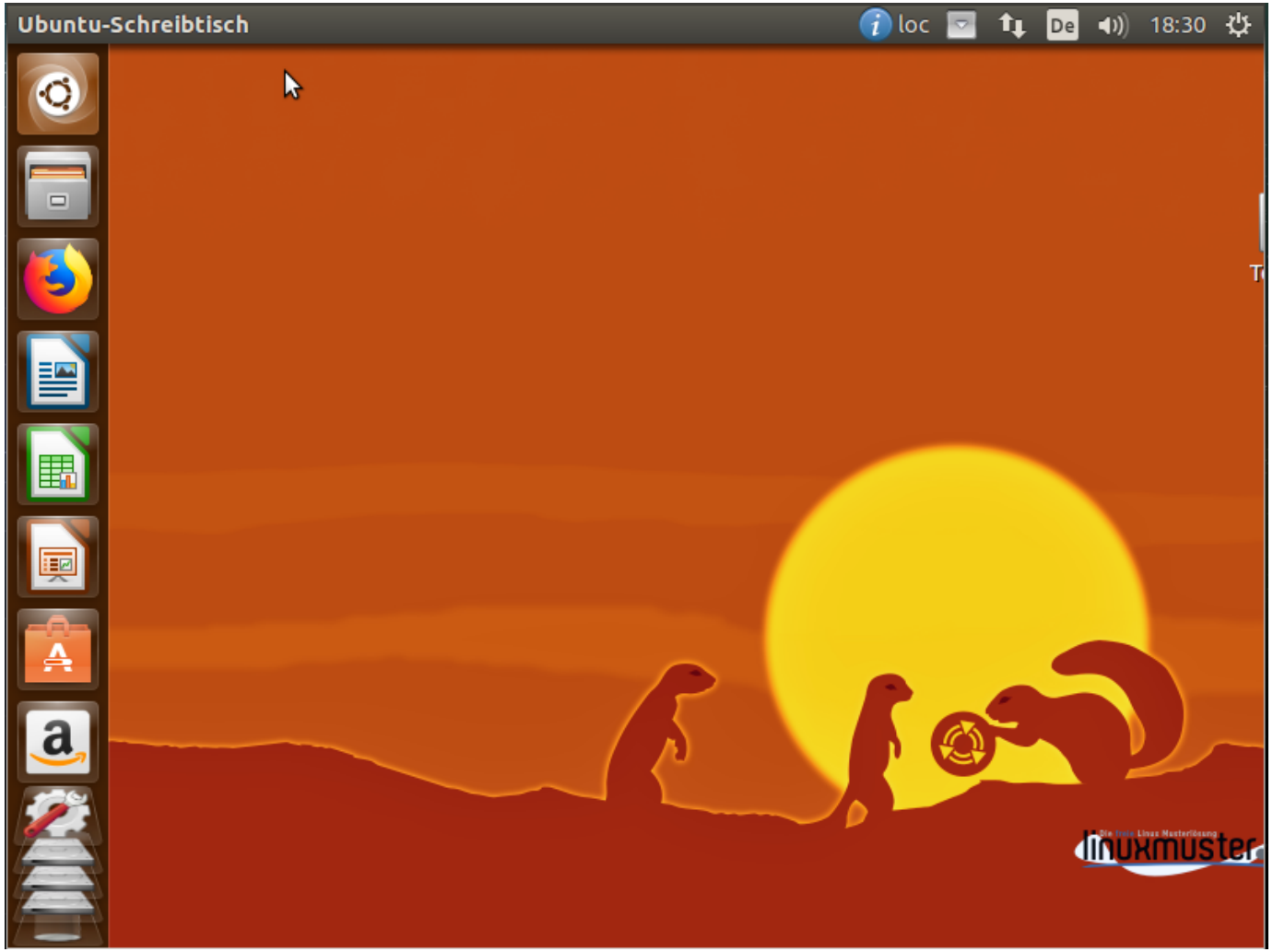


Linbo: Image herunterladen mit rsync (SF)

Linuxmuster Ubuntu 16.04 Client (SF)



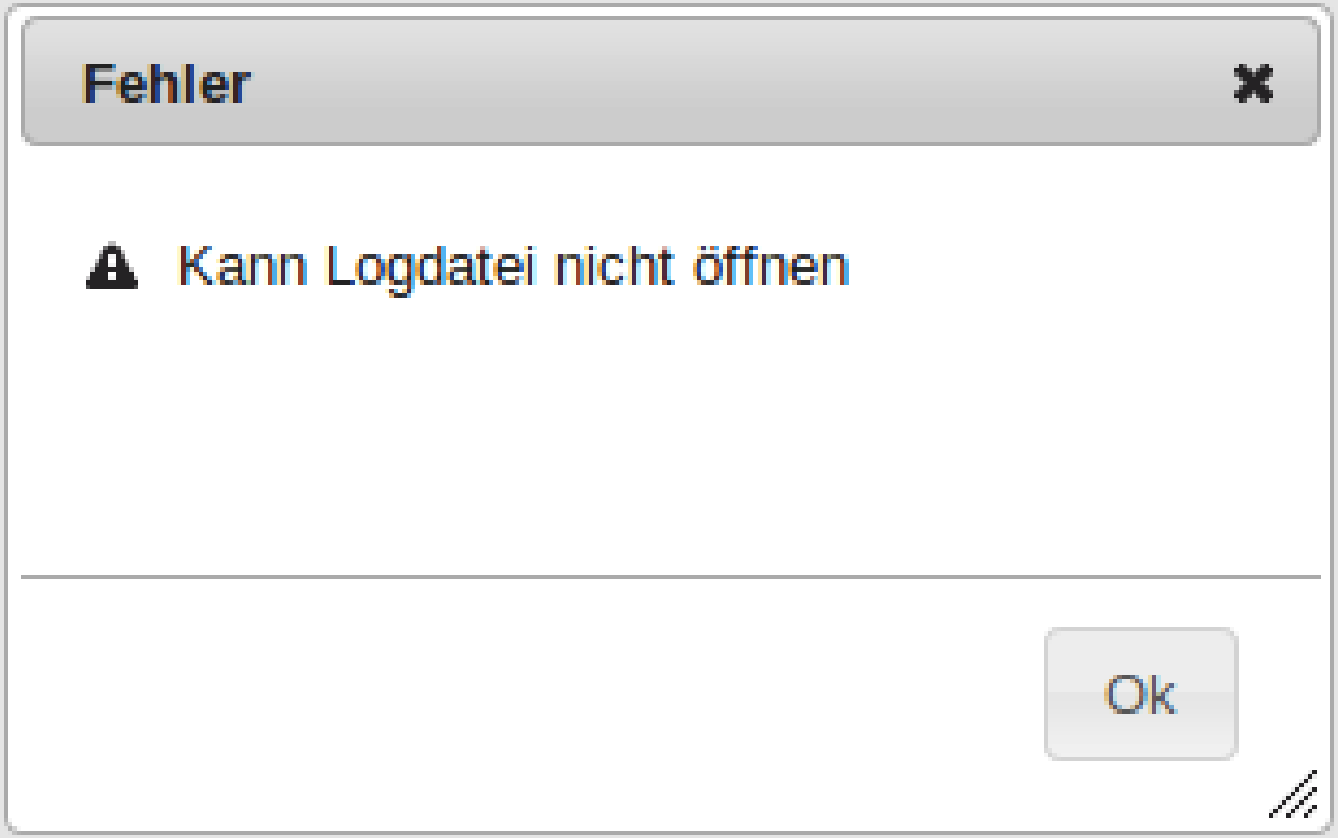
Linuxmuster Ubuntu 16.04 Client (SF)



LM Schulkonsole (SF)

Zugriff nur von eingetragenen Rechnern aus möglich

Hm, und jetzt? (SF)



Grusel (SF)

- Hilfe, Redundanz: Hosts/Lehrer/...stehen im LDAP und in `/etc/linuxmuster/*.txt`
- Server, SSH: `PermitRootLogin yes`
- SMB: `encrypt passwords = true`, *Was ist mit dem Rest?*
- Client nutzt kein `ldaps` für Abfragen
- LDAP: Rechte müssen angepasst werden
  Default: `ldapsearch -x` vom Client aus zeigt (fast) alles
- `$HOME` liegt unverschlüsselt auf HDD
  Abhilfe: ecrytfs/cryfs auf dem Client

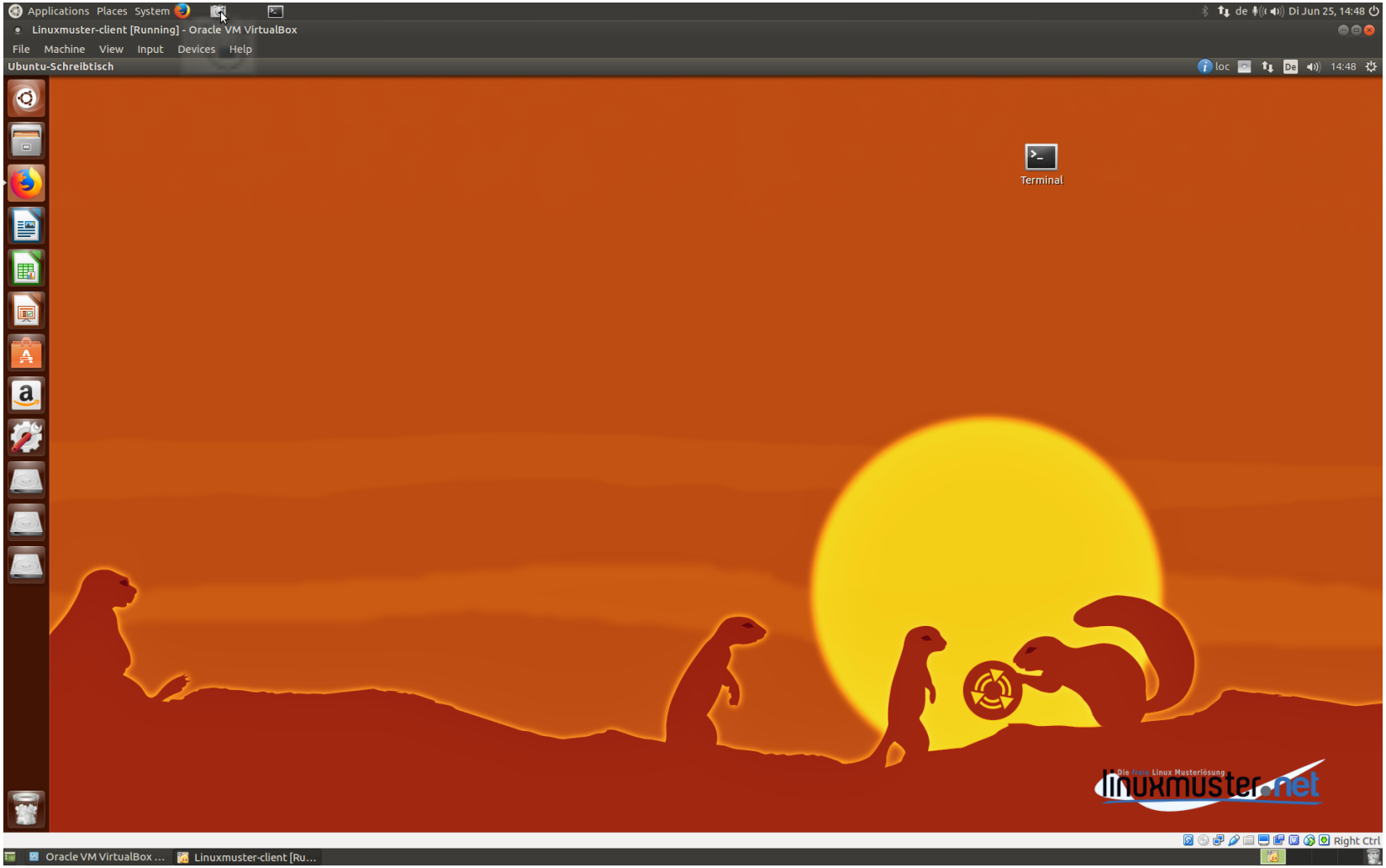
Mozilla: Ohne Worte (SF)

https://t3n.de/news/mozilla-ceo-chris-beard-anbieten-1168614/3/

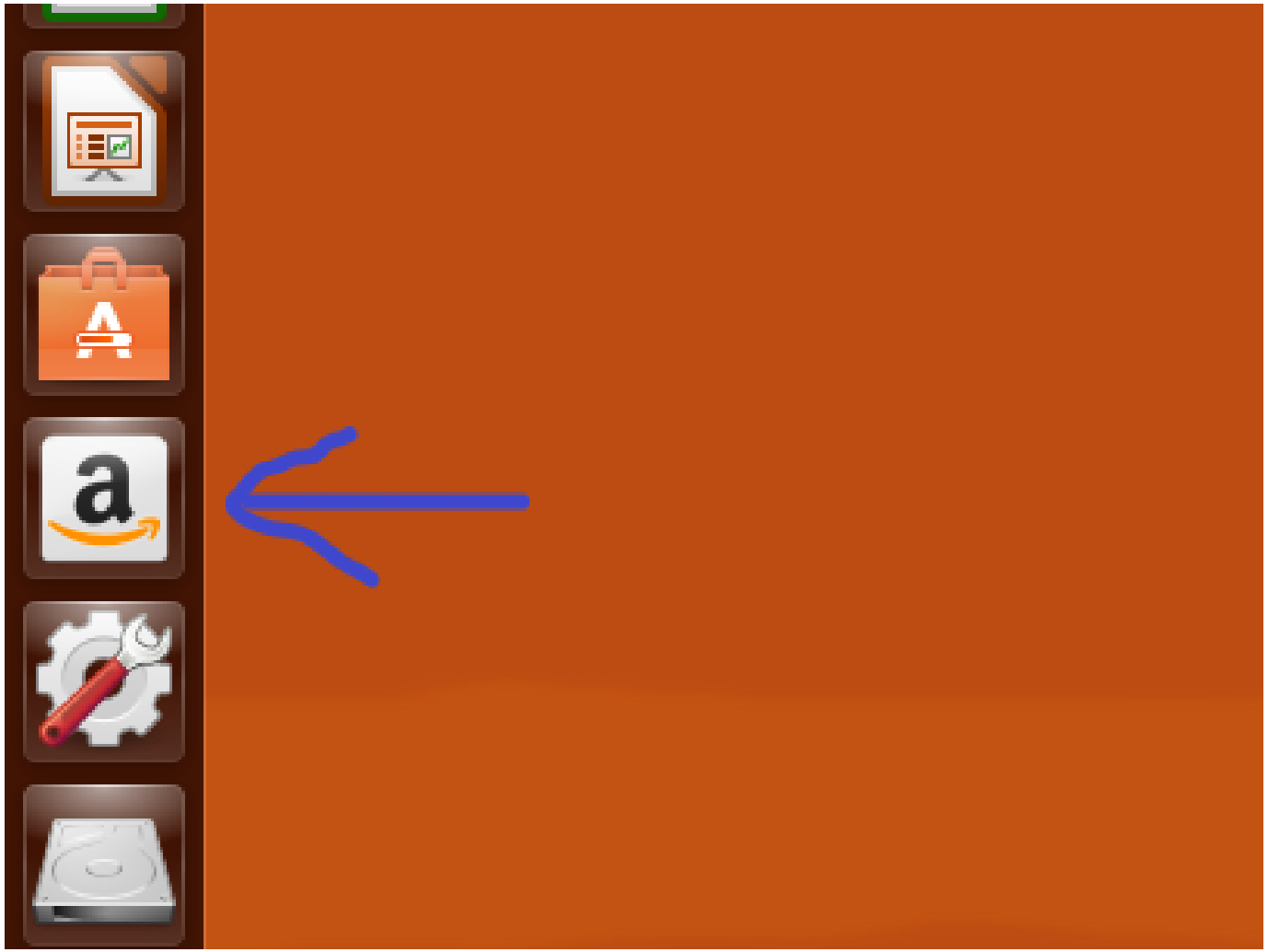
Wir arbeiten an drei Einkommensquellen und wollen sie neu gewichten: Wir haben Search, wir machen aber auch Content. Wir haben eine Firma namens Pocket, die Inhalte entdeckt und kuratiert. Da gibt es auch gesponserte Inhalte. Das ist das Content-Geschäft.
Und das Dritte, an dem wir jetzt arbeiten und was sich entwickelt, während wir über Produkte und Services nachdenken, sind Premium-Ebenen für einige dieser Angebote. Du kannst dir sowas vorstellen wie eine sichere Speicherlösung.

`:%s/firefox/palemoon/g?`

LM 6.2 Ubuntu 16.04 Client: Datenschutz (LK)



LM 6.2 Ubuntu 16.04 Client: Datenschutz (LK)



LM 6.2 Ubuntu 16.04 Client: Datenschutz - Browser (LK)

Applications Places System
Linuxmuster-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Einstellungen - Mozilla Firefox
Einstellungen
Firefox about:preferences#privacy

In Einstellungen suchen

- Allgemein
- Startseite
- Suche
- Datenschutz & Sicherheit
- Firefox-Konto
- Erweiterungen & Themes
- Hilfe für Firefox

Streng
Alle von Firefox erkannten Elemente zur Aktivitätenverfolgung blockieren. Einige Websites funktionieren dann eventuell nicht richtig.

Benutzerdefiniert
Entsprechend den Einstellungen blockieren:

Websites eine "Do Not Track"-Information senden, dass die eigenen Aktivitäten nicht verfolgt werden sollen
Weitere Informationen
- Immer
- Nur wenn Firefox bekannte Elemente zur Aktivitätenverfolgung blockieren soll

Cookies und Website-Daten
Die gespeicherten Cookies, Website-Daten und der Cache belegen derzeit 6,2 MB Speicherplatz. Weitere Informationen

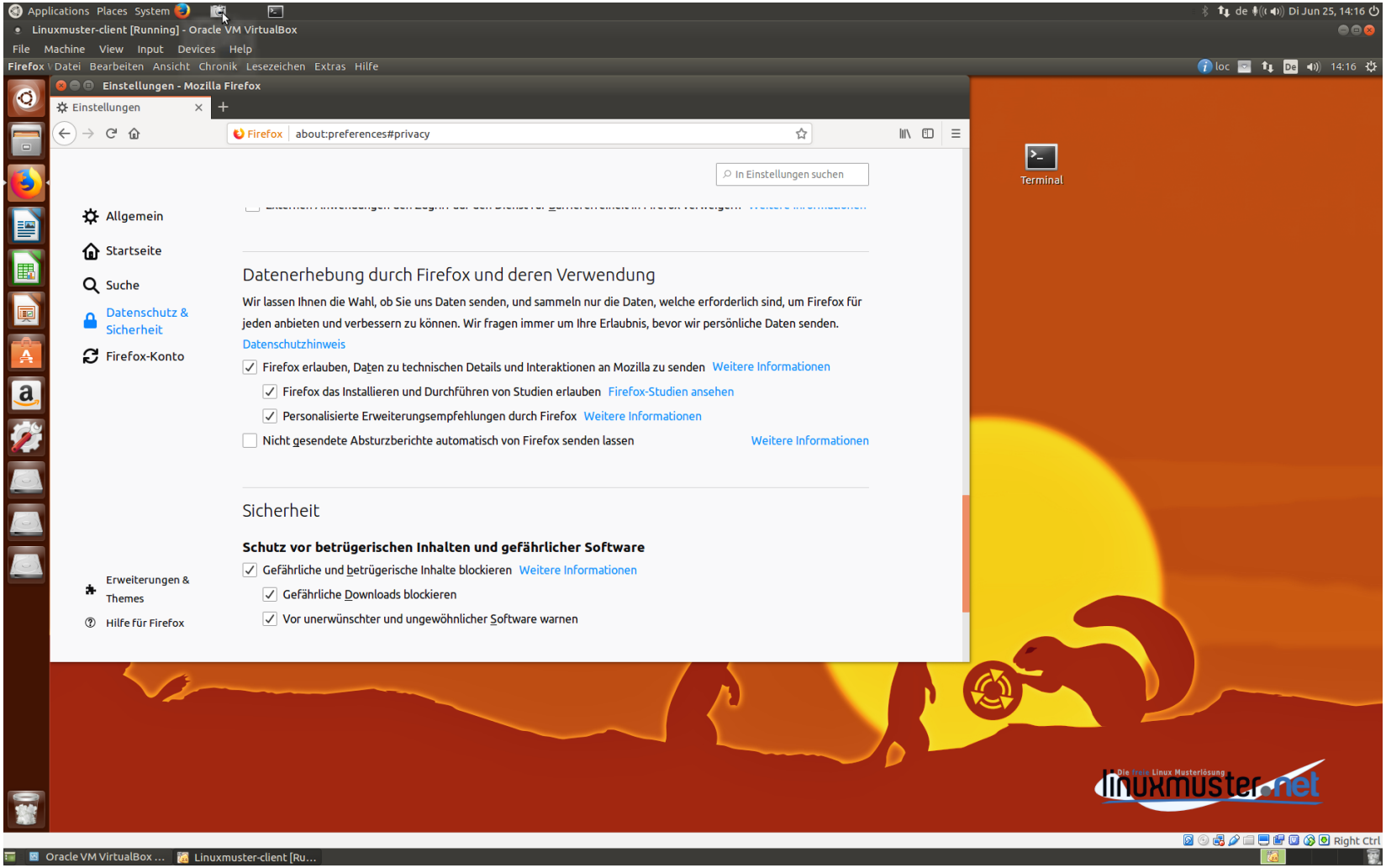
Daten entfernen...
Daten verwalten...
Cookies und Website-Daten beim Beenden von Firefox löschen
Berechtigungen verwalten...

Zugangsdaten & Passwörter

Terminal

Oracle VM VirtualBox ... Linuxmuster-client [Ru...

LM 6.2 Ubuntu 16.04 Client: Datenschutz - Browser (LK)



LM 6.2 Ubuntu 16.04 Client: Datenschutz - Browser (LK)

Wie funktioniert der Betrugsversuch- und Schadprogrammschutz in Firefox?

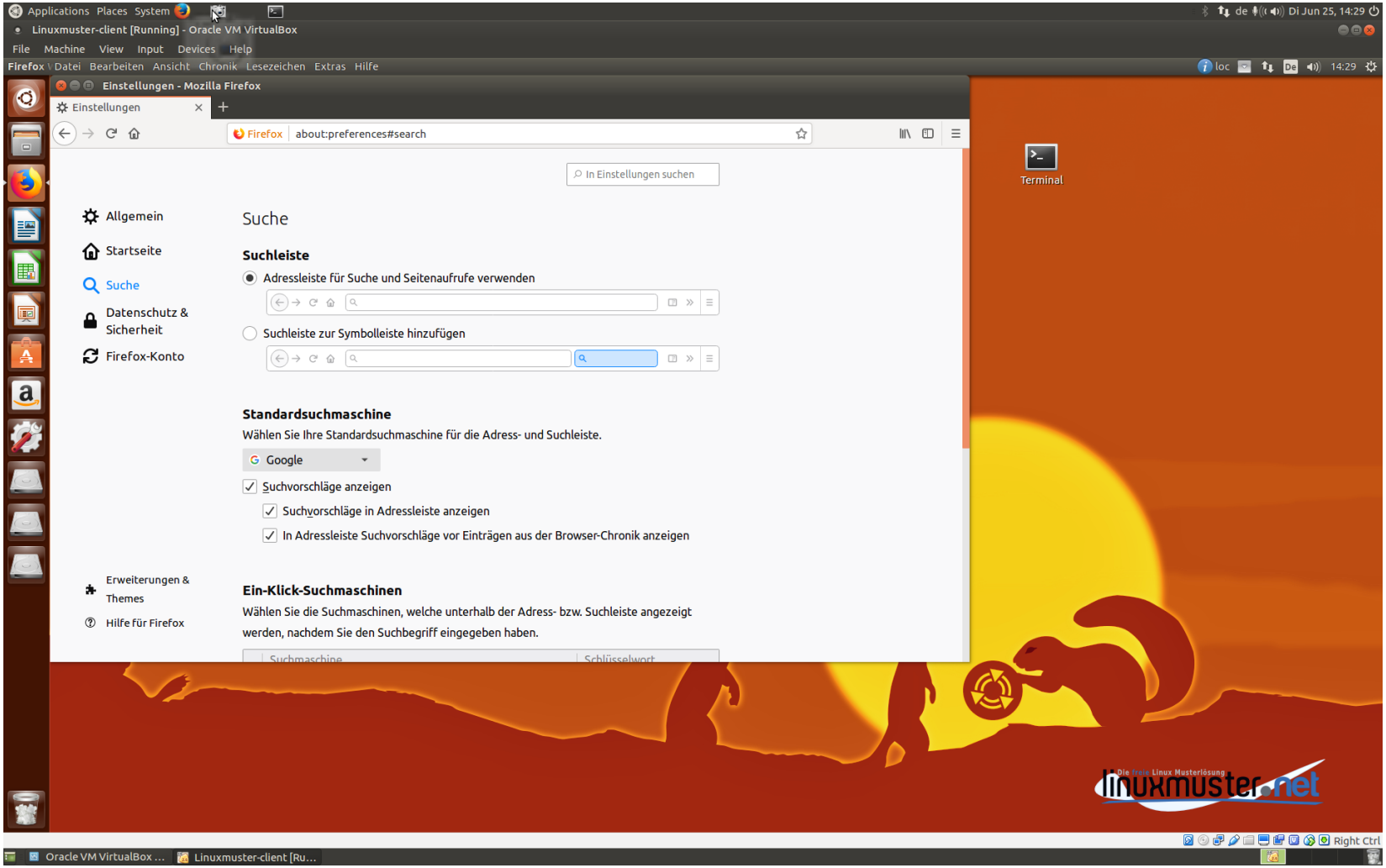
Der Betrugsversuch- und Schadprogrammschutz überprüft jede Webseite darauf, ob sie bereits in einer Liste mit Betrugsversuchen, Schadseiten oder unerwünschter Software enthalten ist. Diese Listen werden alle 30 Minuten automatisch aktualisiert, wenn die Schutzfunktion aktiviert ist.

Beim Herunterladen einer Anwendung überprüft Firefox, ob der Download von einer Seite stammt, die bekanntermaßen Malware verteilt, und blockiert in diesem Fall den Zugriff. Ansonsten fragt Firefox beim „Safe Browsing Service“ von Google an, ob die Software sicher ist, indem einige Metadaten des Downloads dorthin übermittelt werden.

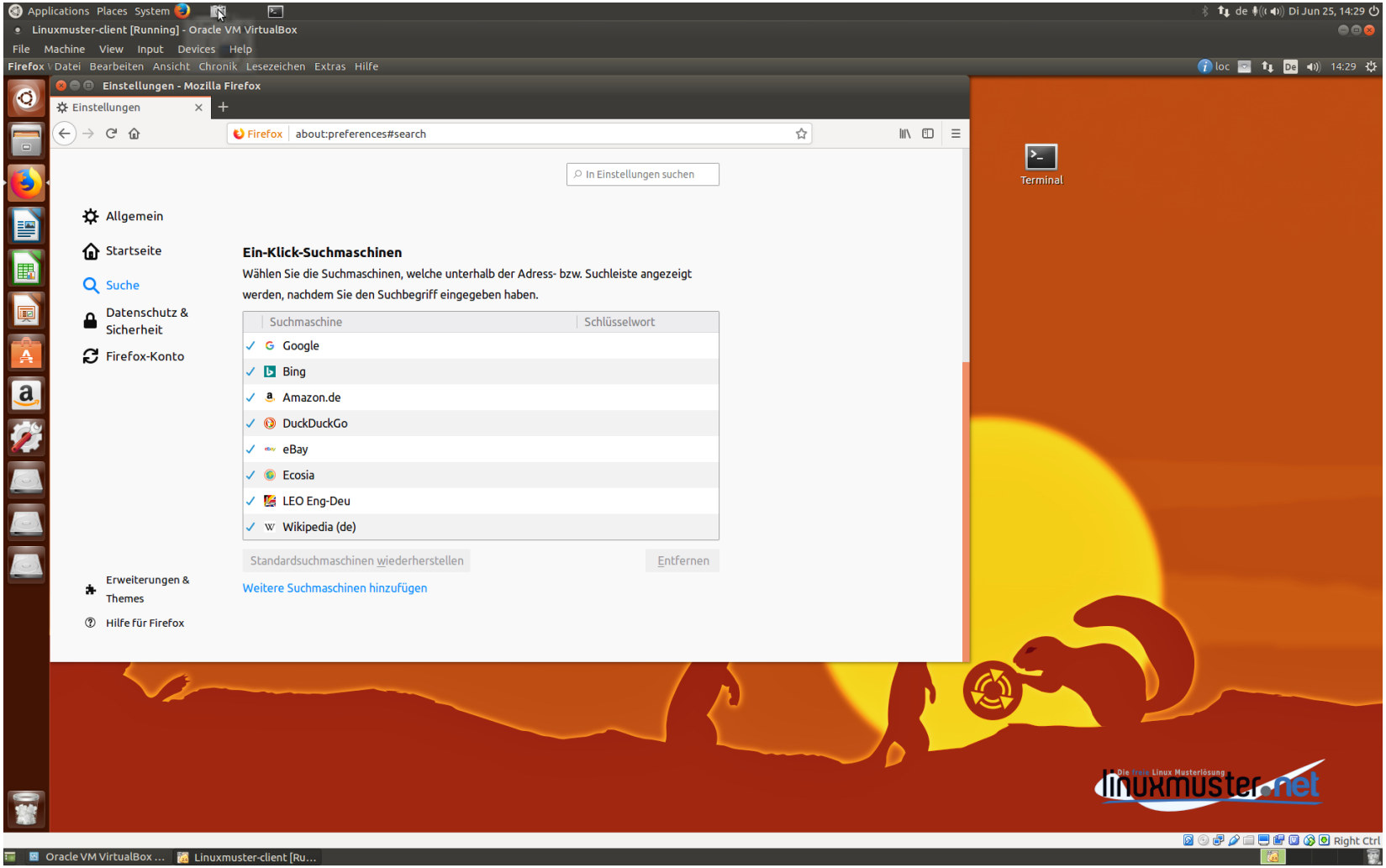
LM 6.2 Ubuntu 16.04 Client: Datenschutz - Browser (LK)

- "Do Not Track" kann zwar von Trackern ignoriert werden, sollte aber dennoch aktiv sein
- Mozilla macht den Eindruck immer Daten hungriger zu werden
- Datenerhebung deaktivieren

LM 6.2 Ubuntu 16.04 Client: Datenschutz - Suche (LK)



LM 6.2 Ubuntu 16.04 Client: Datenschutz - Suche (LK)



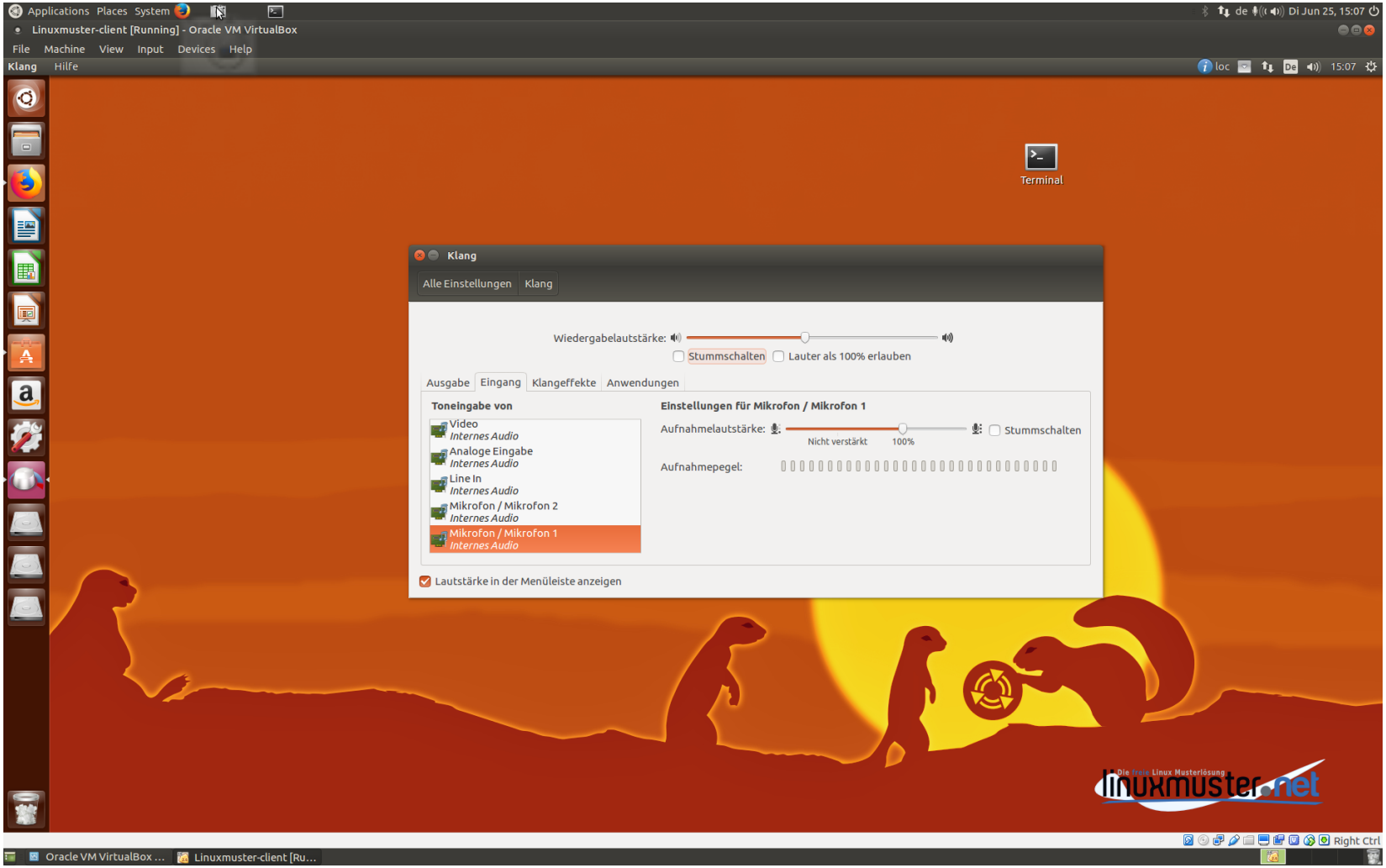
LM 6.2 Ubuntu 16.04 Client: Datenschutz - Suche (LK)

- Standartsuchmaschine ist Google
- Muss geändert werden da Alphabet größtes Werbeunternehmen und damit Datensammler
- Auf dict.leo.org laufen Skripte von google-analytics.com und amazon-adsystem.com
- Für andere Suchmaschinen ausführliche Informationen auf https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen
- Von installierten Suchmaschinen nur Wikipedia unbedenklich

LM 6.2 Ubuntu 16.04 Client: Datenschutz - Suche (LK)

- Alternativen:
- MetaGer.de (Spendenfinanziert)
- Qwant.com (Anonymisierte Ergebnisse von Bing)
- startpage.com (Anonymisierte Ergebnisse von Google)
- qwantjunior.com und blinde-kuh.de für Kinder

LM 6.2 Ubuntu 16.04 Client: Datenschutz - Kamera (LK)



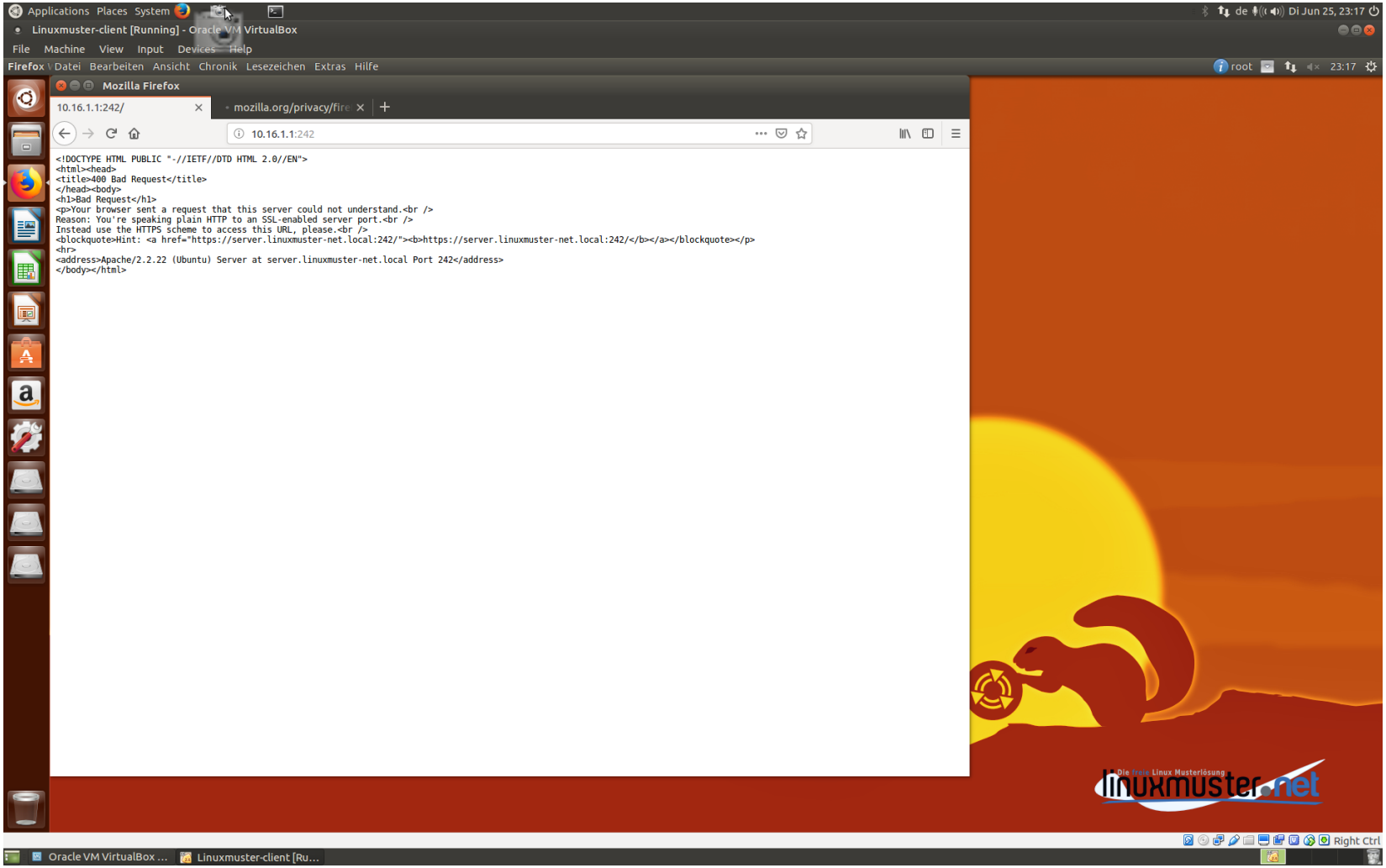
LM 6.2 Ubuntu 16.04 Client: Datenschutz - Kamera (LK)

- Große Gefahren für Kinder, wenn sie Aufnahmen von sich anfertigen können und möglicherweise verbreiten
- Mikrofon kann einfach in Einstellungen aus und ein geschaltet werden
- Kameratreiber mit lsmod/ lsusb finden
- Siehe auch wiki.ubuntuusers.de/Webcam
- Wie im LM_Kompass beschrieben deaktivieren
- Wiedereinschalten benötigt dann root-Rechte

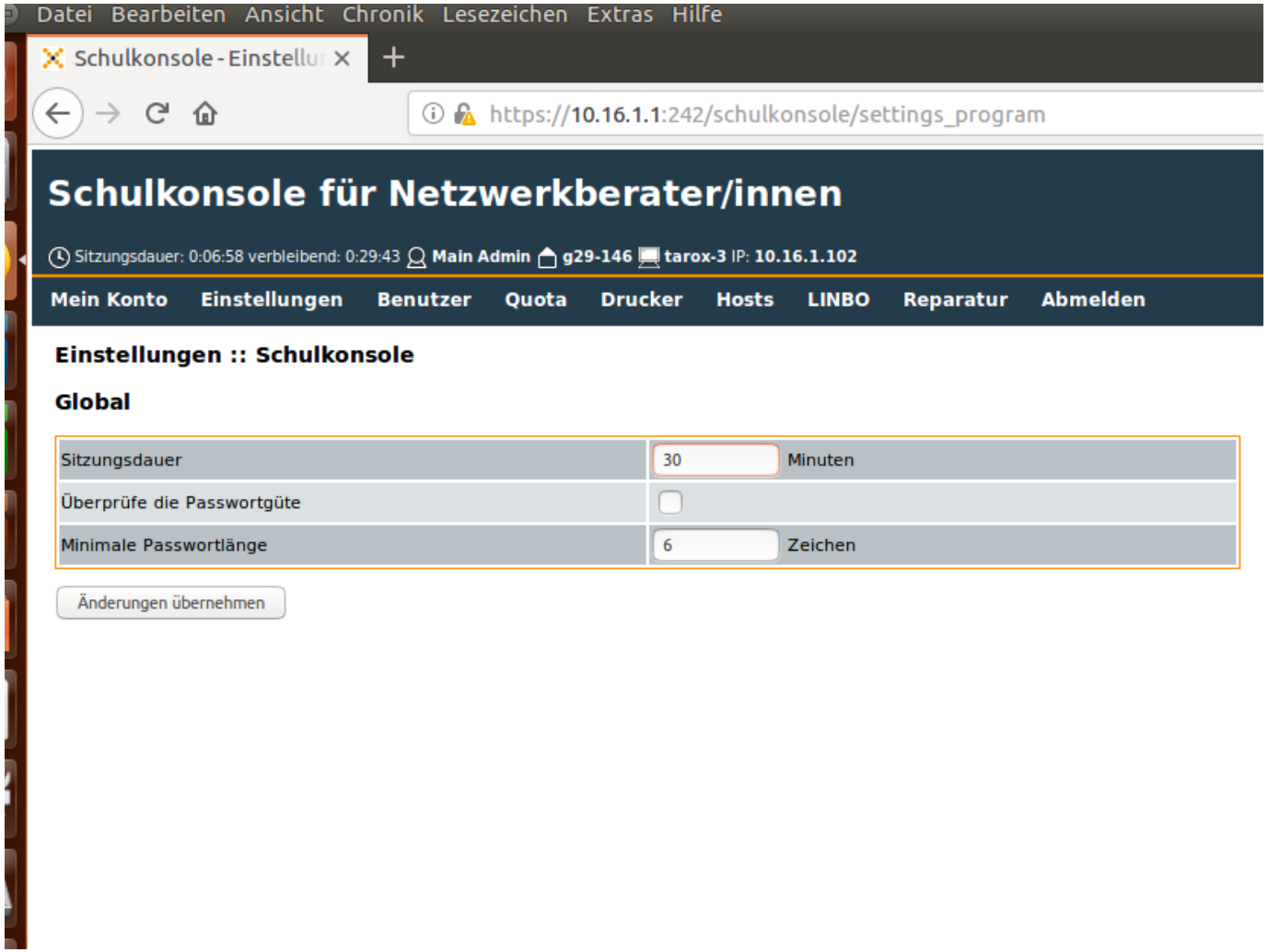
LM 6.2 Ubuntu 16.04 Client: Datenschutz - Apps (LK)

- Problematische Apps entfernen:
  - Google Maps
  - Cheese (Videos mit Webcam machen)
- Neu hinzufügen:
  - Openstreetmaps

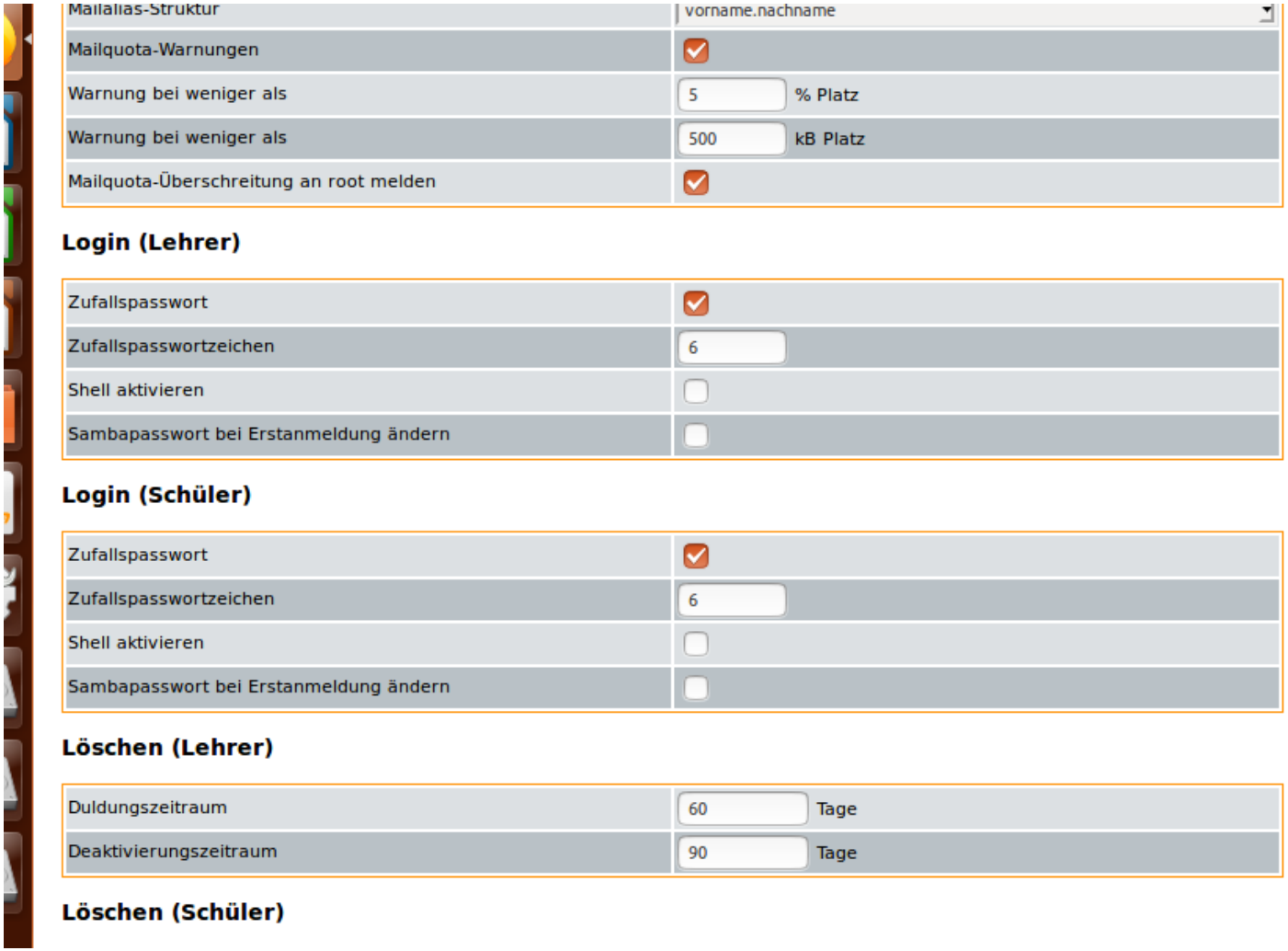
LM 6.2 Schulkonsole: Datenschutz (LK)



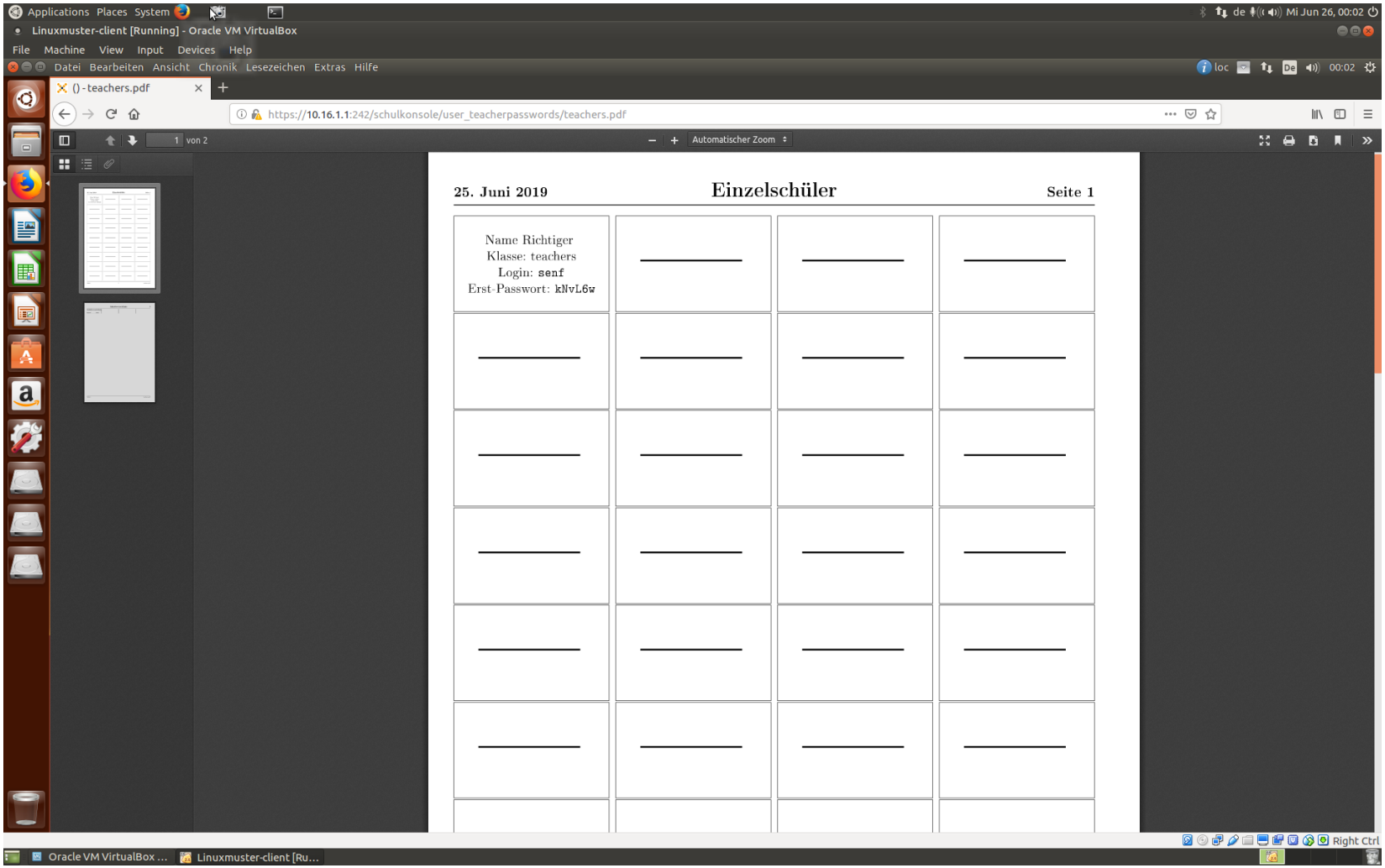
LM 6.2 Schulkonsole: Datenschutz (LK)



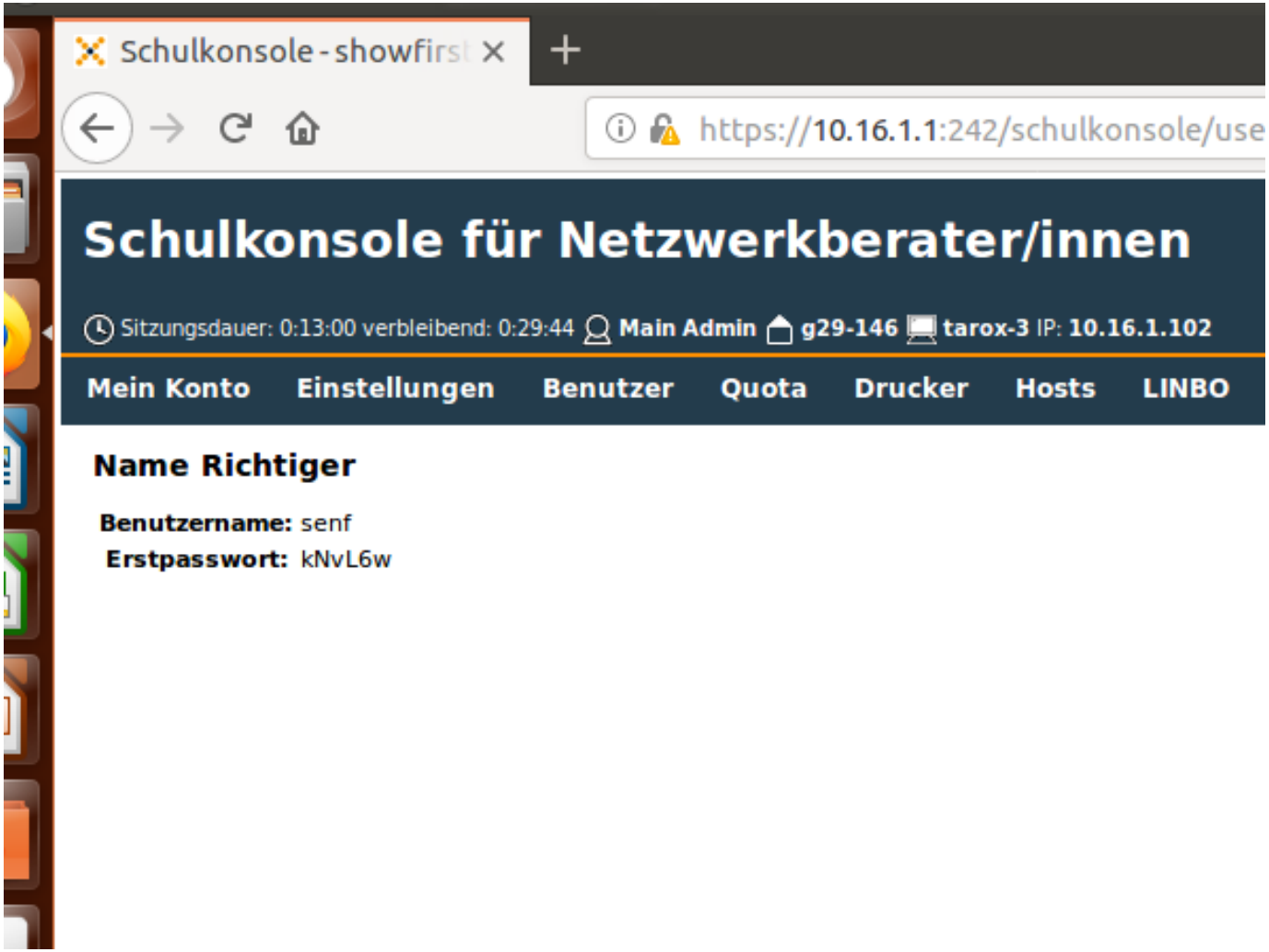
LM 6.2 Schulkonsole: Datenschutz (LK)



LM 6.2 Schulkonsole: Datenschutz (LK)



LM 6.2 Schulkonsole: Datenschutz (LK)



LM 6.2 Ubuntu 16.04 Client (LK)

- Client aktuell halten
- apt-get upgrade

Linuxmuster-Kompass (LK)

(1)Clients

- Nutze wenn möglich den Linux-Client
- Deaktiviere das Mikrofon:
  Einstellungen>Klang>Eingang
- Kameratreiber deaktivieren; unter
  ect/modprobe.d/blacklist.conf
  blacklist „Treibername, z.B. uvcvideo"
  https://www.linux-community.de/ausgaben/linuxuser/2015-09/leserpost-tipp-ue/
- TODO: Telemetrie Ubuntu16.04
- Anti-Virus-Programme nur für Windows sinnvoll!
- Sensibilisiere die Nutzer für das Thema Datensicherung!
- Datensicherung nur kurzzeitig anschließen.
- Sicherung auf DVD schützt vor Ransomware.

Entferne Amazon aus dem Starter!

(2) Internetbrowser und Suchmaschine

- Passe Firefox unter Privacy-Gesichtspunkten an!
  https://privacytools.io/browsers/#firefox-setting-v
- Für Einstellungen about:preferences in Adressleiste eingeben.

Datenschutz und Sicherheit

- „Do Not Track"-Information immer senden!
- Entferne alle Häckchen in der Datenerhebung durch Firefox!

Suche

Entferne alle schnüffelnde Suchmaschinen:
- Google
- Bing
- Amazon.de
- eBay
- Ecosia
- DuckDuckGo

TODO: Browser Adons
- Skript blocker
- Neat-Url
- ect....

(3)Apps(TODO)

- Entferne Google Maps!
- Verwende stattdessen das freie openstreetmaps!
- Entferne Cheese!
- *Hast du den Firefox-Browser schon angepasst?*

TODO: Anpassungen LDAP und SAMBA

Falls Windows Clients benötigt werden besteht erheblicher Anpassungsbedarf! Siehe hierzu den allgemeinen Sec-by-Design Kompass!
Beachte unbedingt auch die Verweise!
Beachte die Kosten und Folgekosten welche durch die Software-Lizenzen entstehen!

Suche

Füge sinnvolle Alternativen hinzu:
- Startpage.com
- MetaGer.de
- blinde-kuh.de

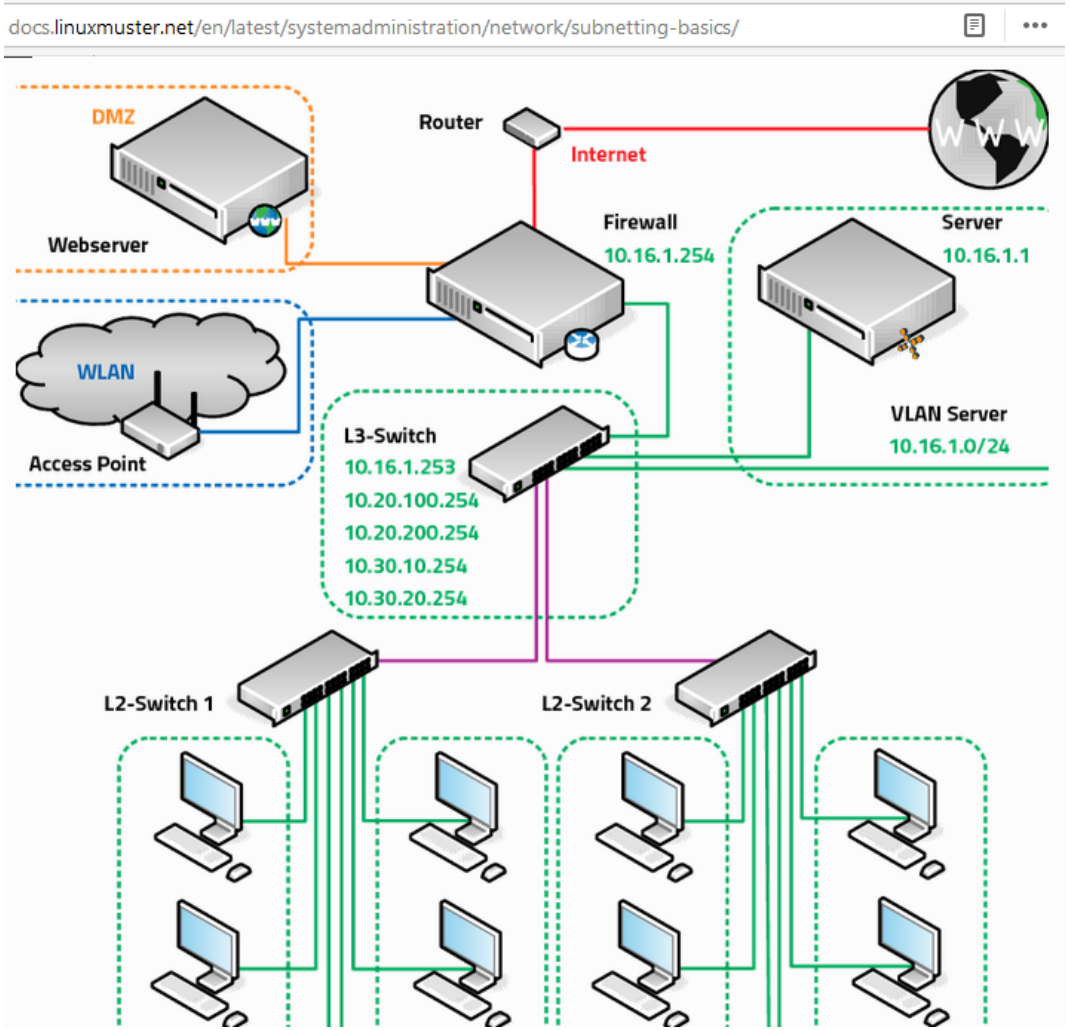
Setze Standartsuchmaschine für Kinder im Grundschulalter auf blinde-kuh.de!
Informiere dich über aktuelle Änderungen!
https://digital.wdr.de/digitale-welt/sicherheit-gut-gut-geht-auch-ohne-google-bei-der-suche-im-internet

TODO: Verschlüsselung in Thunderbird integrieren

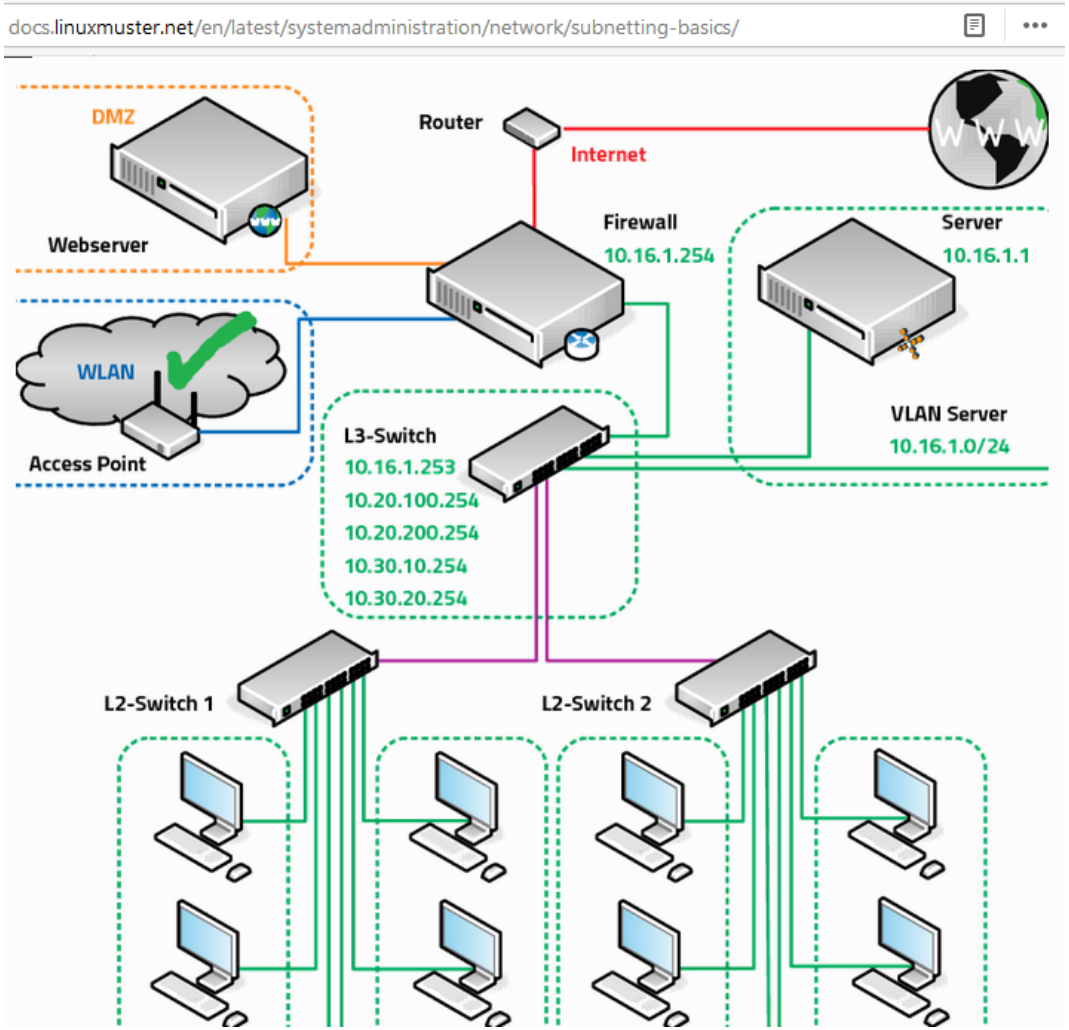
TODO: Server

Sichere regelmäßig den Server mit
`linuxmuster-migration-backup`
https://www.linuxmuster.net/de/dokumentation/backup-und-restore-tipps

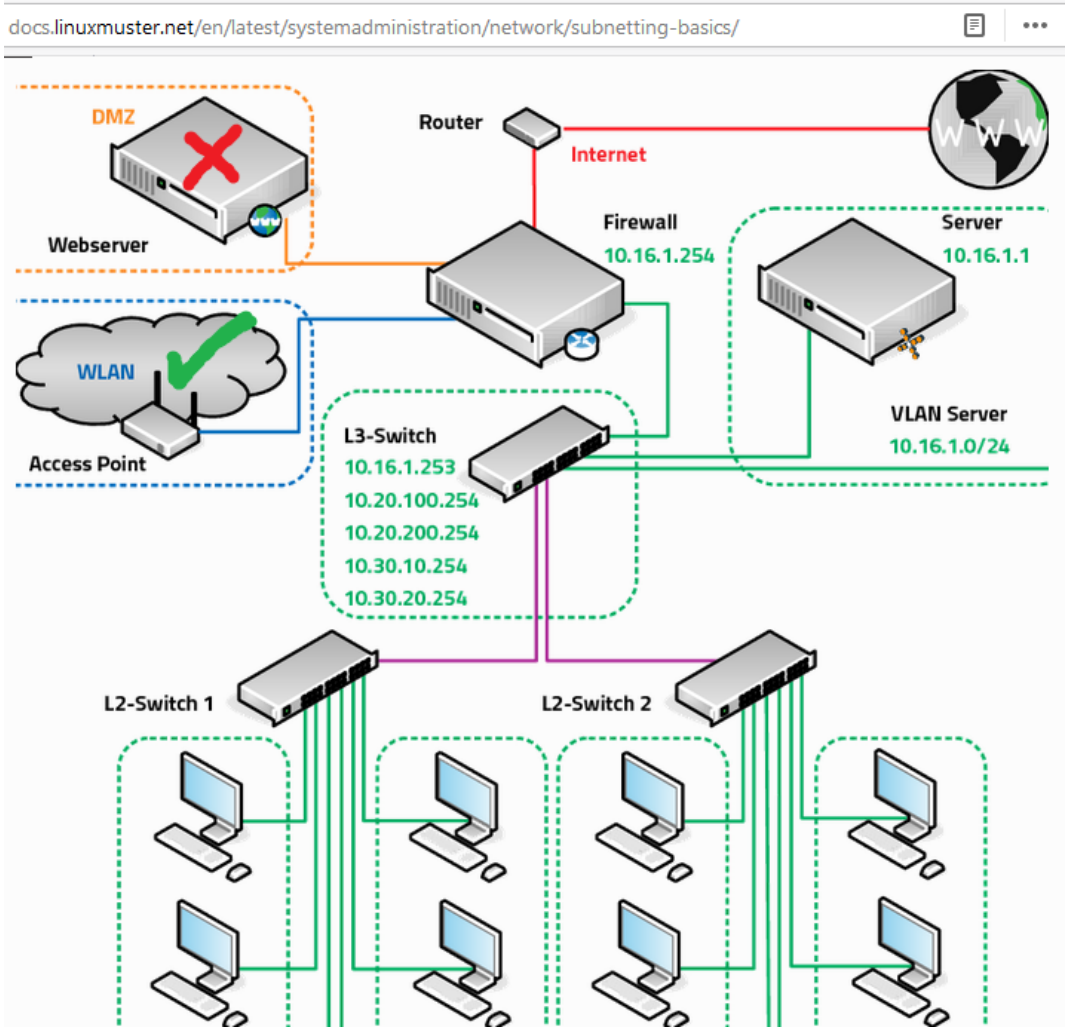
Netzarchitektur (N.N.)



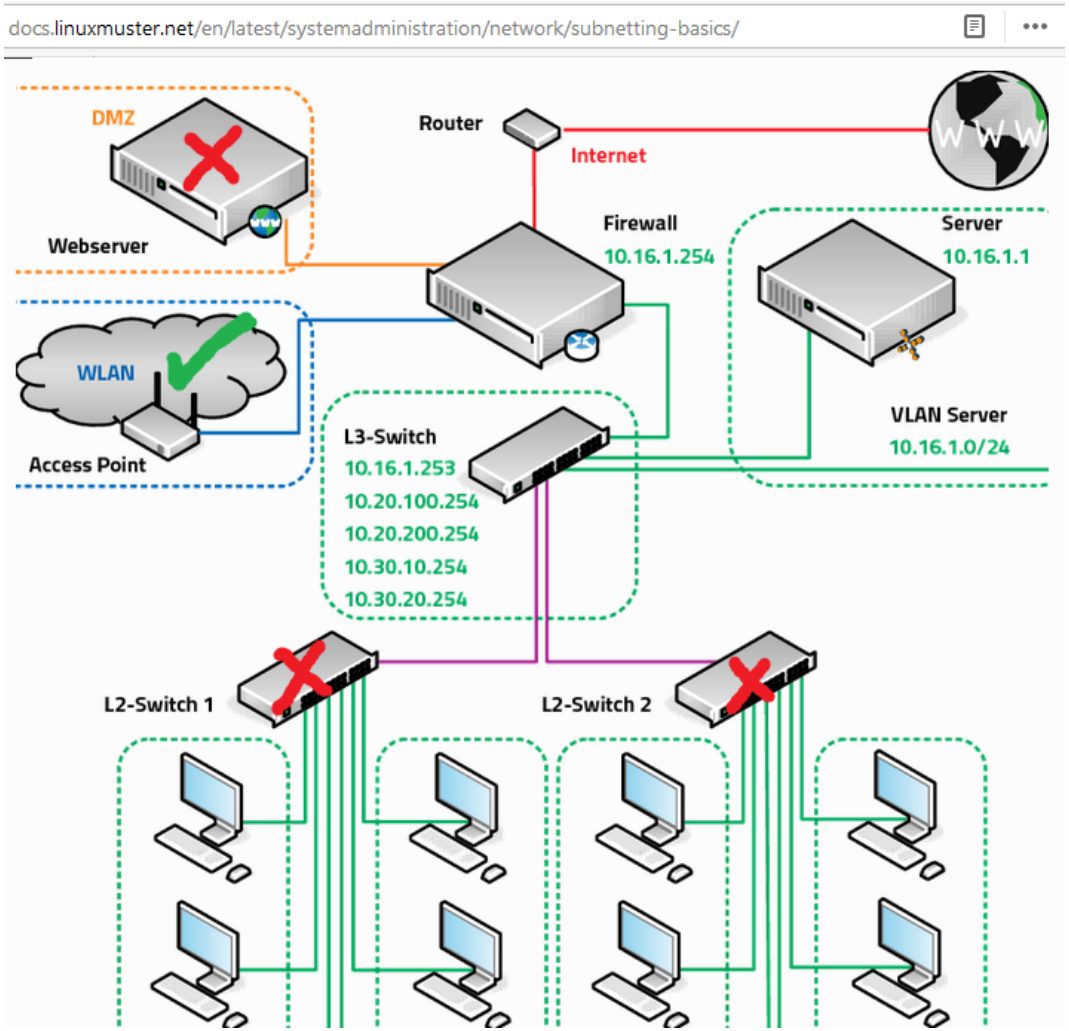
Netzarchitektur (N.N.)



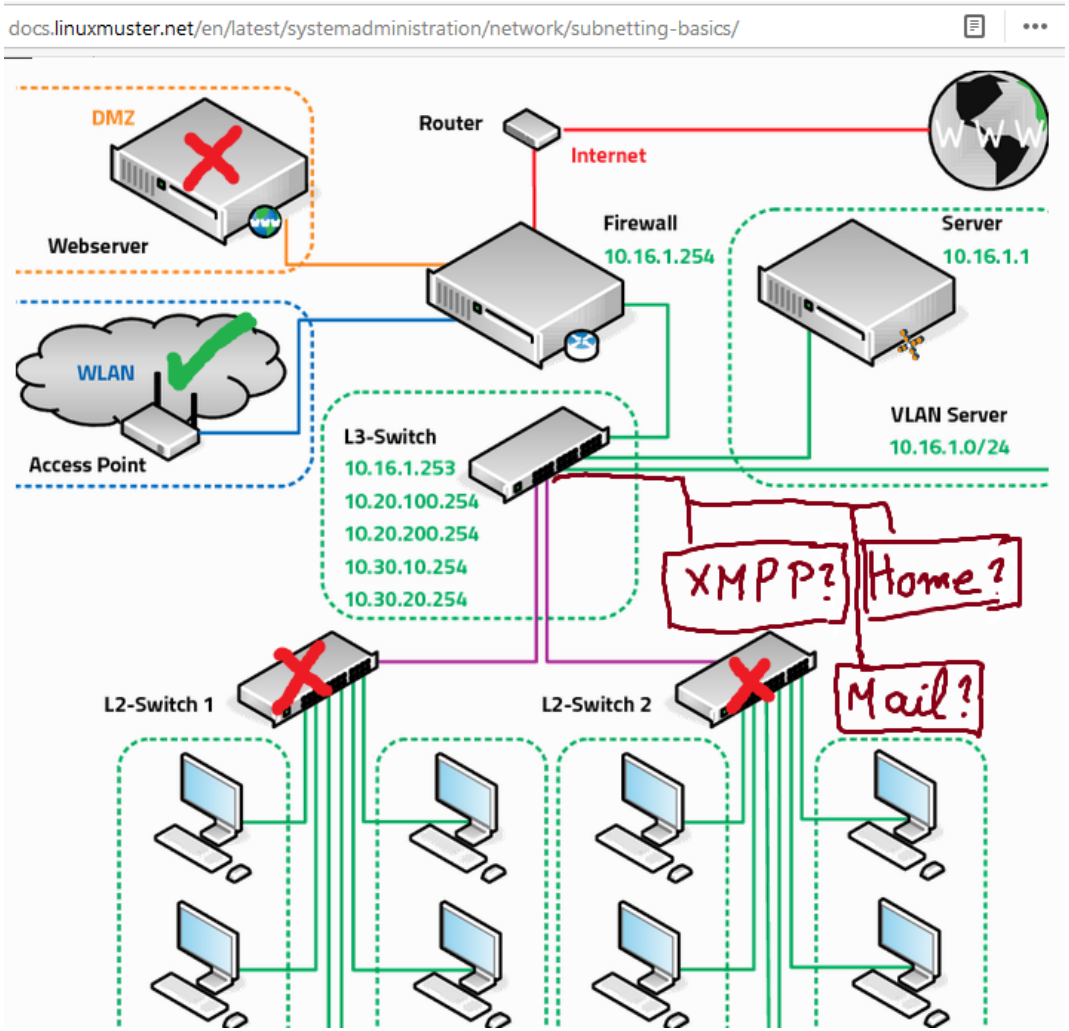
Netzarchitektur (N.N.)



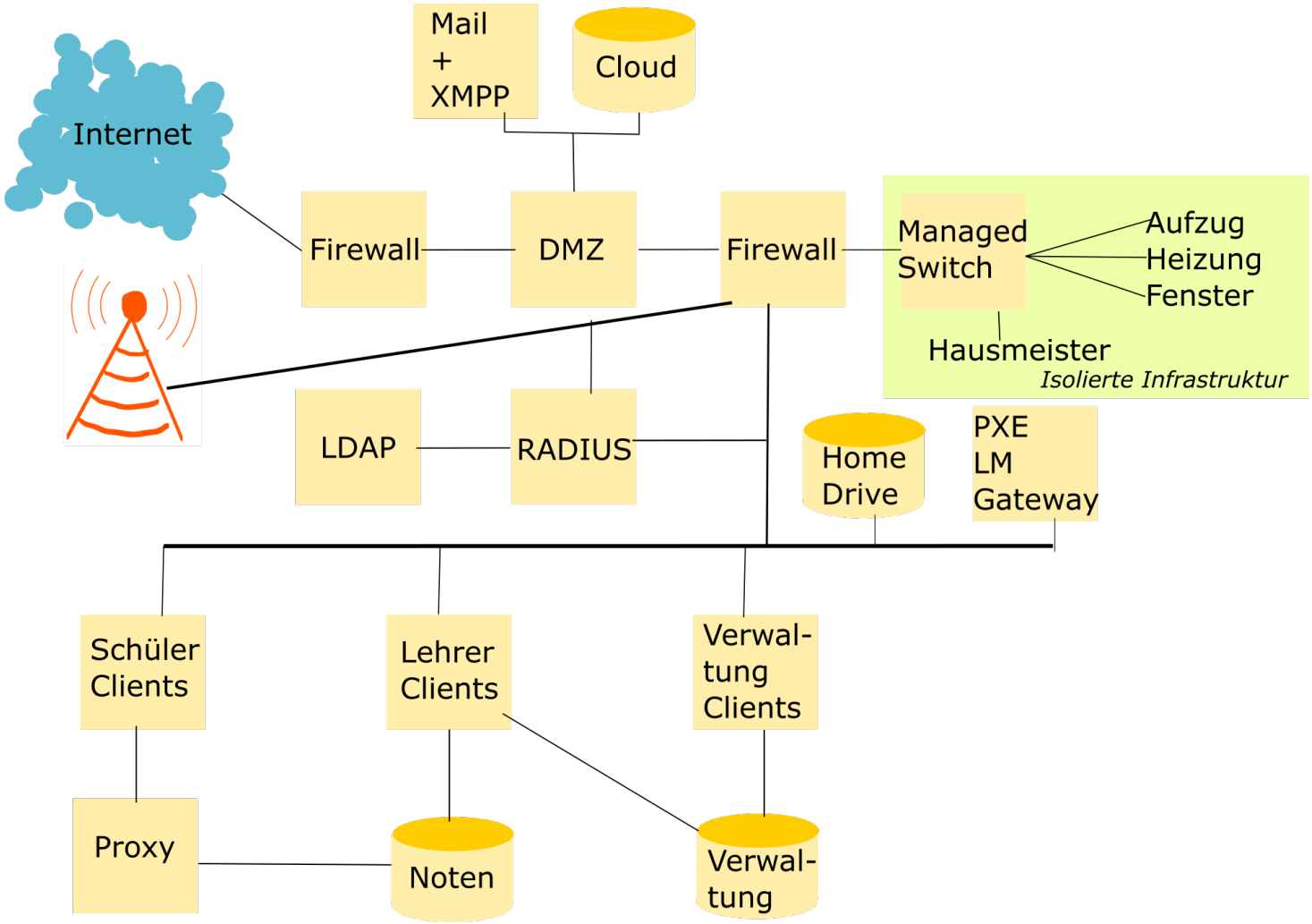
Netzarchitektur (N.N.)



Netzarchitektur (N.N.)



Netzarchitektur (N.N.)



Zusammenfassung (SF)

- Rechte der Schüler müssen respektiert werden
- Andere Projekte (MSN oder Puavo) riechen irgendwie
- LM ist cool: freiwillige Community, starker FLOSS-Gedanke
- LM hat noch viele Bugs und Schwachstellen, Dokumentation noch rudimentär
- Es steht bereits: LM 6.2 Server, LM 6.2 Default Client, Test-CA

Probleme während des Projektes (SF)

- Zu wenig Zeit
- Virtualisierung des Servers mit Virtualbox erfolglos, kostete uns mehrere Wochen
  VBox generell gruselig (Host-IO-Cache `off` → Guest-`ext4` geht kaputt)
- Während des Projektes: Anpassungen bei LM, da Vorbereitungen für LM 7.0
- Dokumentation nicht aktuell und stellenweise rudimentär, Screenshots oft aus alten Versionen

Was muss noch getan werden? (SF)

- 2FA einrichten: Zertifikate ins LDAP, PAM-Module für Client und Server, Smartcard-Unterstützung für Clients
- Ab LM 7.0: Samba 4, bringt Kerberos mit (KDC Isolation?)
- Nextcloud einrichten, Samba-Shares einbinden und 2FA, Mailserver und XMPP-Server einrichten
- Client Images: Datenschutzkonform machen, Multimedia-Fähigkeiten untersuchen
- Moodle einrichten und integrieren

Wenn Interesse: Zusammenarbeit mit LM-Entwicklerteam erwägen